Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 12-13-2016	**2. REPORT TYPE** Final Technical Report	**3. DATES COVERED** *(From - To)* 5-13-2015 to 8-16-2016

4. TITLE AND SUBTITLE: **Scalable Engineering of Quantum Optical Information-Processing Architectures (SEQUOIA)**	**5a. CONTRACT NUMBER** W31-P4Q-15-C-0045 **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S): Dr. Saikat Guha; Dr. Dirk Englund; Dr. Karl Berggren	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)Ma Raytheon BBN Technologies 10 Moulton Street Cambridge, MA 02138 Massachusetts Institute of Technology 77 Massachusetts Avenue Cambridge, MA 02139	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) US Army Army Contracting Command Redstone Arsenal, AL Defense Advanced Research Projects Agency DSO Arlington, VA	**10. SPONSOR/MONITOR'S ACRONYM(S)** US Army ACC-RSA, DARPA DSO **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
DARPA-funded research: BAA 14-46, DSO Office-wide

14. ABSTRACT
The goals of this seedling program were to analyze requirements on key devices and algorithms to realize scalable photonic quantum information processing (QIP) systems that can significantly outperform classical / conventional computing methods. Specifically, we investigated resources requirements for linear optical quantum computing to achieve scalable quantum computation and a detailed resource-cost vs. performance study for using all-optical quantum computing to build quantum repeaters for long-range quantum-secured communications (viz., QKD).

15. SUBJECT TERMS
DARPA, optical information processing, single photon detectors

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Saikat Guha, Ph.D.
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	U	132	**19b. TELEPHONE NUMBER** *(include area code)* 617-873-5122

13 December 2016

“Scalable Engineering of Quantum Optical Information-Processing Architectures (SEQUOIA)”

Final R&D Status Report
Reporting Period: 13 May 2015 - 16 August 2016

Sponsored by
Defense Advanced Research Projects Agency (DOD)
DSO

Issued by
U.S. Army Contracting Command – Redstone
Contract No. W31P4Q-15-C-0045

Agent
U.S. Army RDECOM, Aviation & Missile Research, Development & Engineering Center

Contract Number:	W31P4Q-15-C-0045
Proposal Number:	P14265-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Saikat Guha
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Contract Period of Performance:	13 May 2015 – 16 August 2016
Total Contract Amount:	$448,405
Total Amount Expended:	$446,550

DISCLAIMER

“The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency, the U.S. Army, or the U.S. Government.”

Final Report

US Army Contract No: W31P4Q-15-C-0045

Title: Scalable Engineering of Optical Information-processing Architectures (SEQUOIA)

Principal Investigator: Saikat Guha, BBN

Co-PIs: Dirk Englund, MIT and Karl Berggren, MIT

Lead Institution: Raytheon BBN

DARPA Program Manager: Dr. Prem Kumar

Abstract

The goals of this seedling program were to analyze requirements on key devices and algorithms to realize scalable photonic quantum information processing (QIP) systems that can significantly outperform classical / conventional computing methods. Specifically, we investigated resources requirements for linear optical quantum computing to achieve scalable quantum computation and a detailed resource-cost vs. performance study for using all-optical quantum computing to build quantum repeaters for long-range quantum-secured communications (viz., QKD).

On the experimental side, we investigated advanced photonic integrated circuit (PIC) technology, scaling of on-chip superconducting single-photon detectors, and requirements for feedforward. This work showed that silicon photonic circuits can enable new generations of quantum-limited detectors within the next few years, and that an all-optical scalable architecture of quantum computing is a promising approach, but also realized that photonic quantum computing will require the development of several new theoretical and device concepts. Our analysis showed that PIC technologies that could be operated at or near room temperature would bring significant advantages for integration with high-speed digital electronics and room-temperature single photon detector technologies, and we propose a new visible photonics platform based on III-Nitride that is also compatible with complementary metal oxide semiconductor (CMOS) circuits.

On the theory side, we were able to dramatically reduce resource requirements for two key QIP applications: photonic cluster-state quantum computing and photonic quantum repeaters. Our resource analysis on ballistic linear optical quantum computing (LOQC) considered how to build a large continuous "sheet" of optical cluster state that is "connected enough" for universal quantum computing. The sheet of cluster state is prepared by preparing small k-photon cluster states (micro-clusters) and injecting them into a linear optical circuit. At the output, one detects a subset of the modes, and the remainder of the modes carry a resource universal for quantum computing regardless of the measurement results (the measurement results tell us how to use the giant entangled cluster on the remaining unmeasured modes to map any quantum algorithm to it). The

special case of k=1 in the aforesaid way of looking at Ballistic quantum computing is exactly the Aaronson-Arkipov model of boson sampling. Our analysis revealed that a clear trade-off between the size of the input clusters N, and loss tolerance in the circuit, for the final sheet of cluster that comes out to be universal for quantum computing. In particular, by using new techniques from percolation theory, we showed that having k=3 size clusters as a starting resource is a must for loss-tolerant Ballistic LOQC using two-qubit fusion operations. This work establishes, for the first time, a clear trade-space between Aaronson-Arkipov boson sampling, i.e., k=1 (which does not allow universal quantum computing) to photonic cluster states that are universal for quantum computing (i.e., with GHZ states of size $k \geq 3$). k=2 (Bell states) happens to be a border-line case, where Ballistic LOQC is barely possible is all the linear-optic elements are 100% lossless, which of course is impractical. This study tells us that, for scalable LOQC, we need to consider scalable and efficient ways to directly produce $k \geq 3$ size photonic clusters (rather than first producing single photons and probabilistically stitching them together).

We also investigated a special application of all-photonic quantum computing, viz., in building all-optical quantum repeaters for long-distance QKD and entanglement distribution. We investigated what resources are required to beat the best-possible rate achievable without repeaters using photonic quantum repeaters, even when the photonic repeater is constructed using lossy devices (lossy sources and detectors, in-line losses, and coupling losses). We implemented several protocol improvements that reduced physical resources for such schemes by 5 orders of magnitudes from the state of the art at the beginning of the seedling program, to a few million single photon sources per repeater node, or just thousands of GHZ states per repeater station. Towards the conclusion of our seedling program, we further improved the resource requirement by another order of magnitude by developing a "one-way" all-photonic quantum repeater scheme, in collaboration with Prof. Liang Jiang of Yale U., which will be published soon.

The program revealed a highly promising QIP concept based on weak optical nonlinearities. In particular, we demonstrated, for the first time, an approach for a quantum Ising machine based on weak optical nonlinearities. As opposed to currently pursued approaches based on superconducting quantum computing architectures, our all-optical approach could shrink devices by > 5 orders of magnitude, and could operate at room temperature. A similar architecture also holds promise to single-photon nonlinearities at in dielectric cavities that promises circuit-model all-optical quantum computing analogous to superconducting (SC) qubits based quantum computing, but at room-temperature and at optical frequencies.

We developed scalable methods for making and operating arrays of both waveguide-integrated and fiber-coupled superconducting nanowire single-photon detectors (SNSPDs). We also developed high performance SNSPDs on AlN, a wide-bandgap, piezoelectric, and electro-optic semiconductor. SNSPD on AlN can work for a broad spectrum range from UV to mid-IR, and can be potentially combined with other on-chip superconducting electronics to achieve optical modulation. In conjunction with detector development, we also built cryogenic components necessary for large array operation, including cryogenic amplifiers and flexible RF cable bundles.

1. Progress on Experimental Devices and Platforms

1. 1 Demonstration of high-fidelity linear-optics mode transformations

Realizing scalable, high-fidelity interferometric networks is a central challenge to be addressed on the path towards linear optical quantum computation as well as for mediating optical interactions between nonlinear, matter-based qubits. We demonstrated a programmable nanophotonic processor composed of 88 ultra-high contrast Mach-Zehnder interferometers each exhibiting a record extinction ratio exceeding 80 dB, see below. We benchmarked the performance of the processor on single-qubit rotations and showed the first experimental demonstration of a new, error-tolerant universal unitary encoding protocol by implementing 9-dimensional unitary transformations sampled from the Haar measure. We also showed how the fidelity of these transformations can be boosted using in-situ nonlinear optimization techniques. In addition, we introduce new methods for characterizing these large interferometric networks.

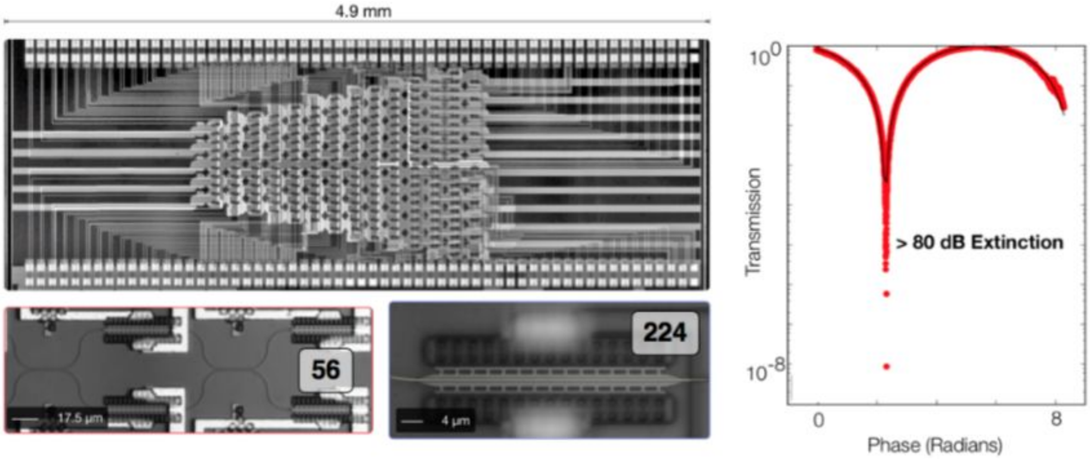


Figure 1:Photonic integrated circuit. Left: programmable PIC. Right: Transmission at one of the output modes, as one of the internal MZI's phase shifters is modulated.

1.2 On-chip nanowire detector array

We developed high-performance NbN nanowire detectors on AlN PICs. These detectors have near-unity quantum efficiency, sub-6-ns reset time, and ~60 ps timing jitter. Since they were fabricated directly on the waveguides, the optical coupling was efficient and low-loss. Figure

2 shows a scanning electron micrograph of AlN waveguide-integrated SNSPDs. The detectors are arranged in such a way that on-chip photon correlation measurement is possible.

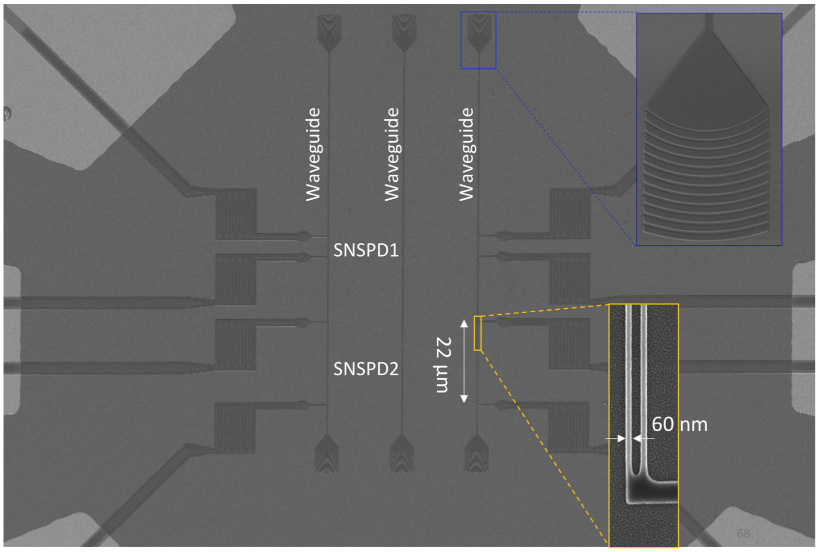


Figure 2: AlN waveguide-integrated SNSPDs.

To read out a large number of detectors, we proposed a time-tagged readout scheme. Figure 3 shows a prototyping time-tagged SNSPD array fabricated on AlN. This array consists of 4 chains, each connecting 16 detectors, which makes a total number of 64 detectors. The time tagging is realized by separating detectors using superconducting slow-wave transmission lines. Impedance matching taper is needed to transform the high-impednace SNSPD to 50 Ω readout electronics. This readout scheme is scalable, and greatly reduces the resources needed for large-array cryogenic readout.

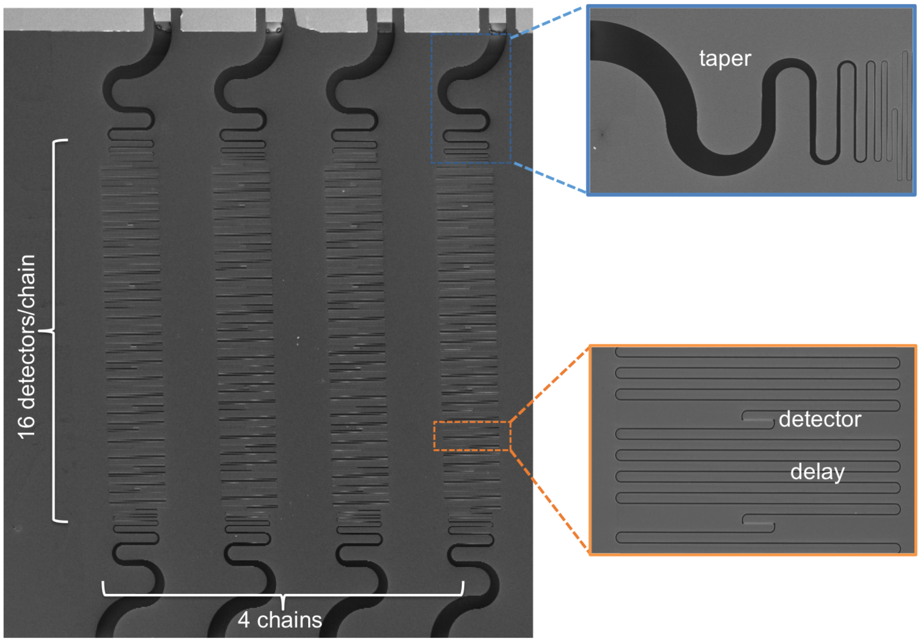


Figure 3: Time-tagged SNSPD array fabricated on AlN. The array consists of 4 detector chains, each connecting 16 detectors in series. Detectors are separated using superconducting slow-wave transmission line, and terminated with impedance-matching tapers to 50 Ω readout circuits.

1.3 Fiber-coupled detector array

Fiber-coupled detector array can be used for off-chip single photon detection. We developed a new packaging technique to couple light from multiple optical fibers to a detector array on a single chip. Figure 4 shows an 8-channel fiber-coupled SNSPD array. The detectors were fabricated on a silicon nitride substrate, and arranged to match the spacing of a commercial fiber array. The fiber array was aligned and glued to the detector chip. These detectors have a circular active area with 15 μm in diameter, and the device yield is > 80%. This packaging technique can be extended to larger array size without much additional effort.

To enable large array operation, we also developed compact cryogenic amplifier and flexible RF cable bundles. These cryogenic components are essential for both waveguide-integrated and fiber-integrated SNSPD arrays.

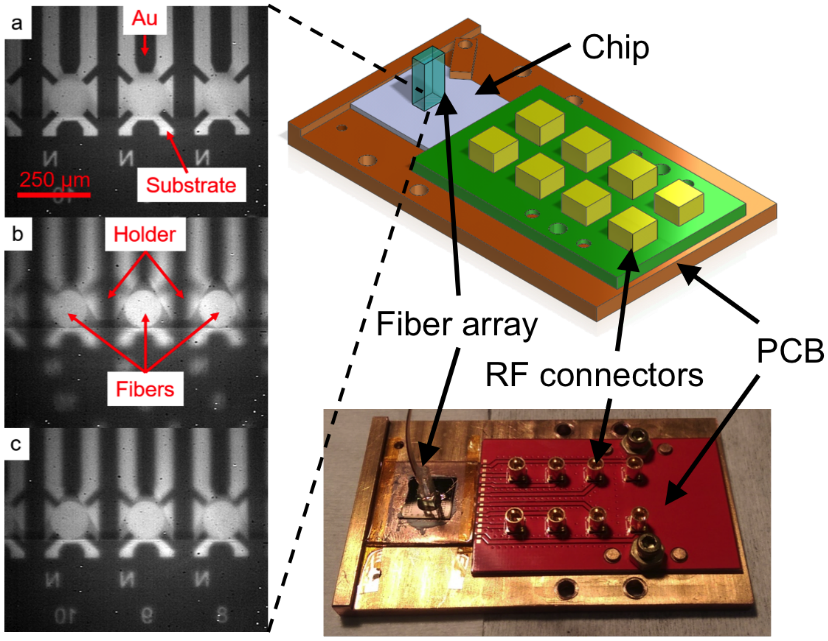


Figure 4: An 8-channel fiber-coupled SNSPD array.

1.4 Post-fabrication-tunable linear optic fabrication

We have analyzed the performance of the programmable nanophotonic processor (PNP) that is dynamically tunable via post-fabrication active phase tuning to predict the scaling of such PICs from tens to hundreds of optical channels. In particular, we have demonstrated that the PNP can perform the mode transformations necessary for a 8x8 Green Machine[1].

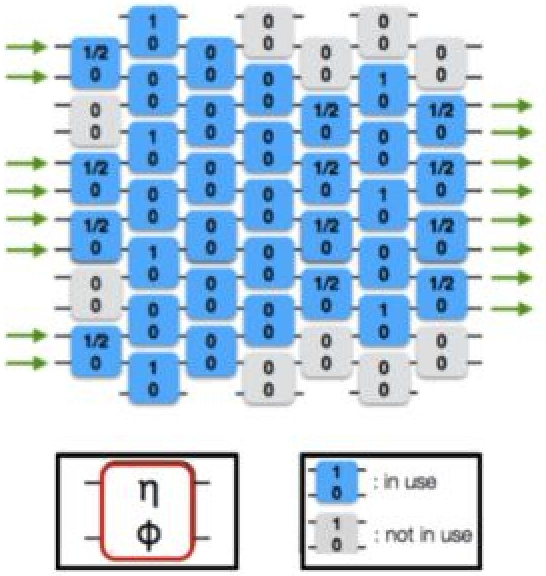


Figure GM1. Green Machine circuit implemented using Mach-Zehnder interferometers in the PNP array configuration.

Building on the development of a circuit (Figure GM1) to implement the Green Machine on the programmable nanophotonic processor (PNP), control hardware and software has been engineered to calibrate the PNP and manipulate light routing within the chip. These features are necessary for configuring the precise phase settings required to demonstrate the Green Machine circuit on a physical chip with non-idealities. Setup and light propagation for the currently controlled PNP, which has 5 input modes and 11 output modes, is shown in Figure GM2.

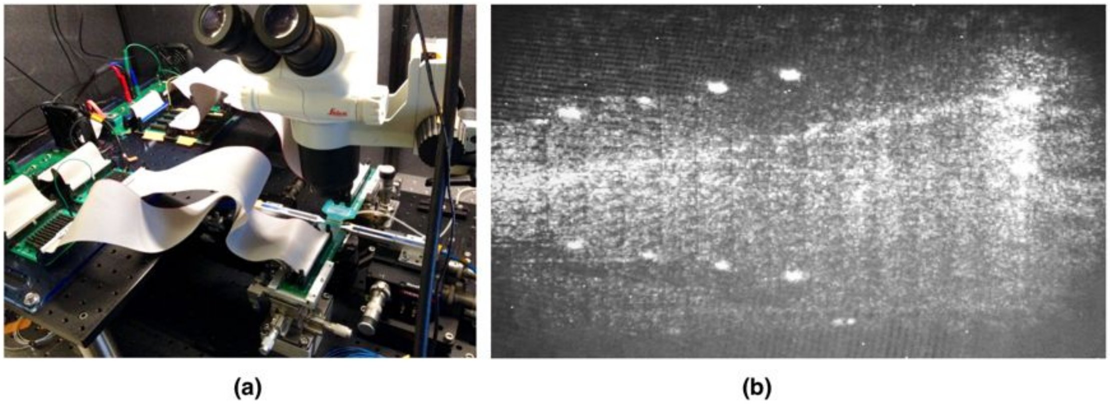


Figure GM2. (a) Hardware control of thermal heater voltages and optical coupling setup for the current PNP chip. Not pictured: photodiode array setup used to detect light coupled from the output waveguides. (b) Propagation of light through the chip, controlled by the setup in (a).

QPP0:

The PNP circuit shown in Figure 1 requires 12 input modes, which is larger than the existing fabricated chip, hereby referred to as QPP0. An alternative test circuit (Figure GM3) was designed to simulate the features of the Walsh transform on QPP0, accounting for the decreased number of input modes. Given that every other output mode on the chip is not routed, the power on only four output modes can be detected simultaneously; therefore, the circuit needed to be altered to read all eight modes from the output. The output probability distribution was measured for this test circuit with very high fidelity, as shown in Figure GM4.

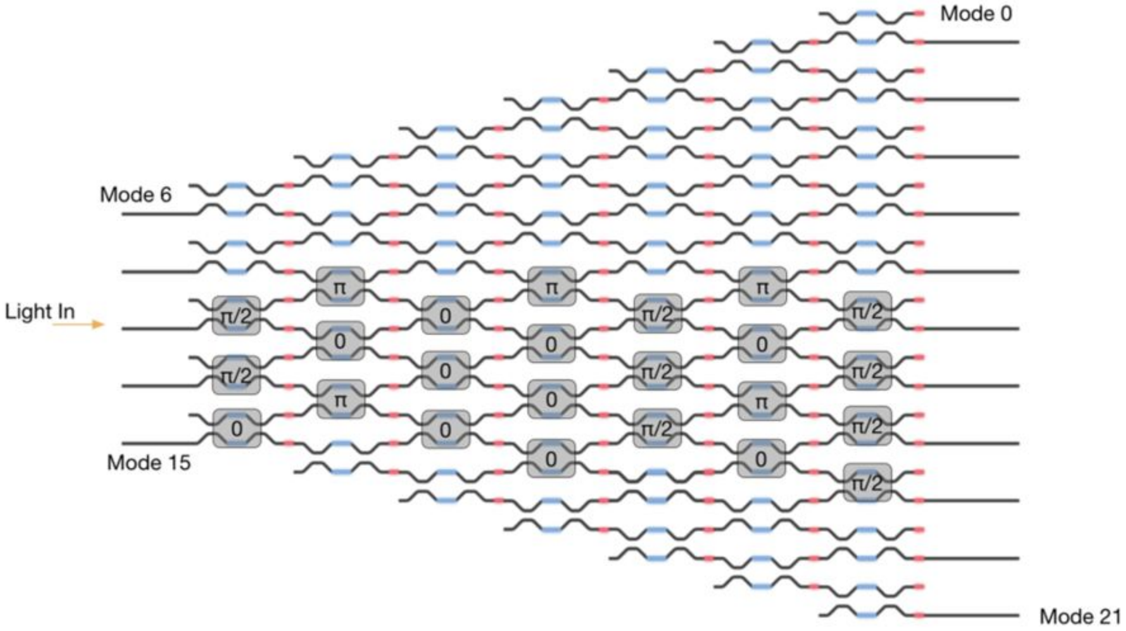


Figure GM3. Test circuit for demonstrating features of the Walsh transform on the compressed QPP0 chip. Mach Zehnder interferometer (MZI) internal arm phase differences are denoted in the gray boxes. Here, π/2 performs a 2x2 Hadamard operation, π performs an identity, and 0 performs a perfect swap.

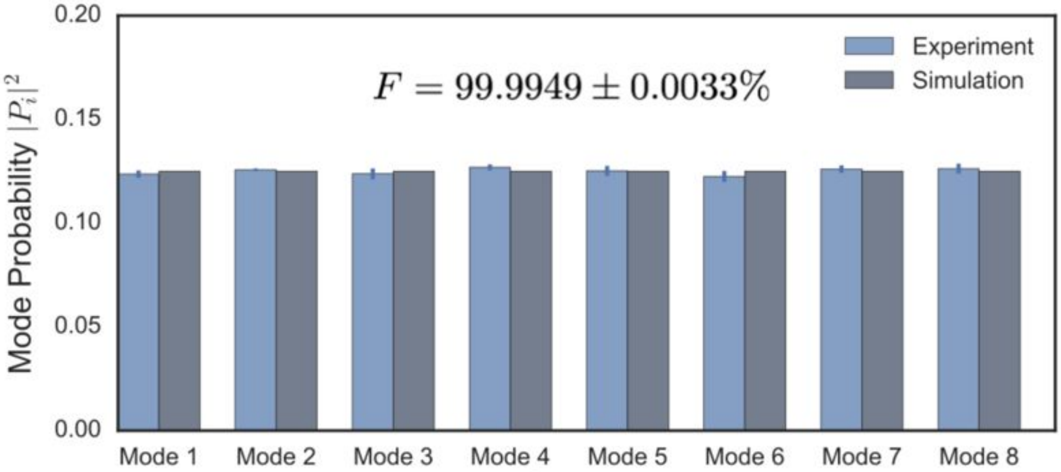


Figure GM4. Output probability distribution of Green Machine test circuit with one excited input mode. Fidelity of the experimental data with respect to software simulations of the circuit yield high fidelity of operation of 99.9949±0.0033%.

PNP1b:

A larger chip, PNP1b, consisting of 26 input modes, 26 output modes, and 176 individually-controlled thermal phase shifters (Figure 5) has been fabricated and packaged. The software for the QPP0 has been designed to be compatible with PNP1b as well. A free space coupling system has been developed and is being tested that, in conjunction with a PID thermal control loop, could enable coupling to and from the chip that is approximately 1dB less than that which can be obtained with standard edge coupling. The free space system makes use of a beam expansion system deployed using two AR-coated lenses, shown in Figure GM6.

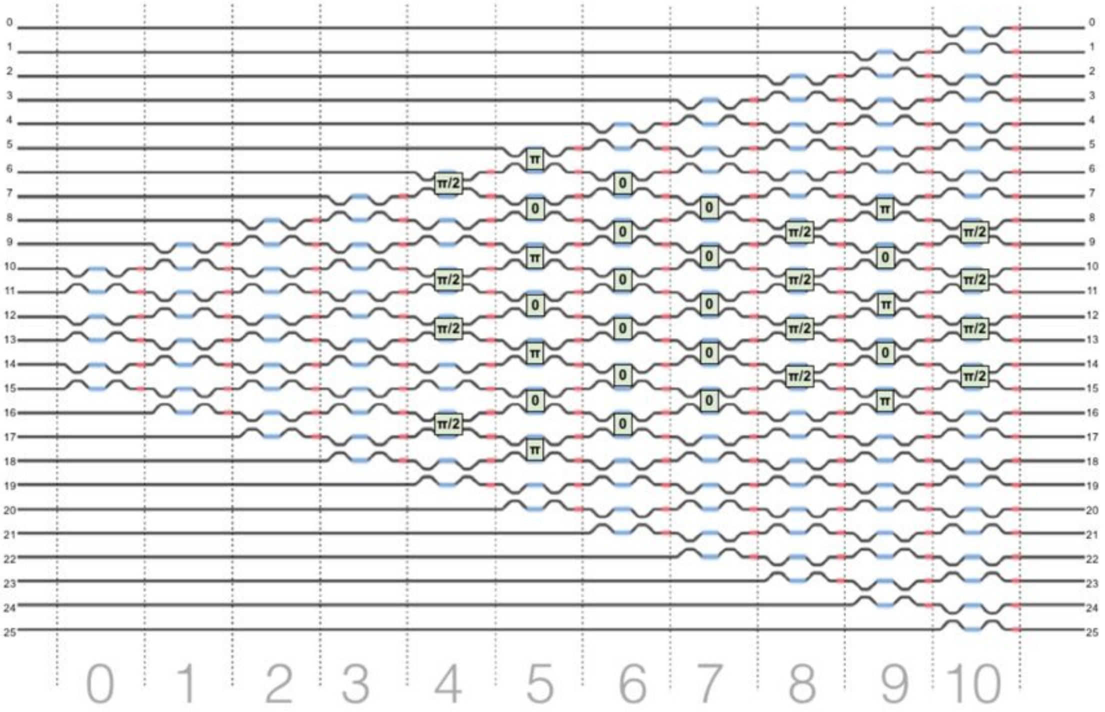


Figure GM5. Layout of the larger 26-mode, 264-heater PNP that is currently packaged. MZI internal phase settings corresponding to an implementation of the Green Machine circuit are shown in the shaded boxes.

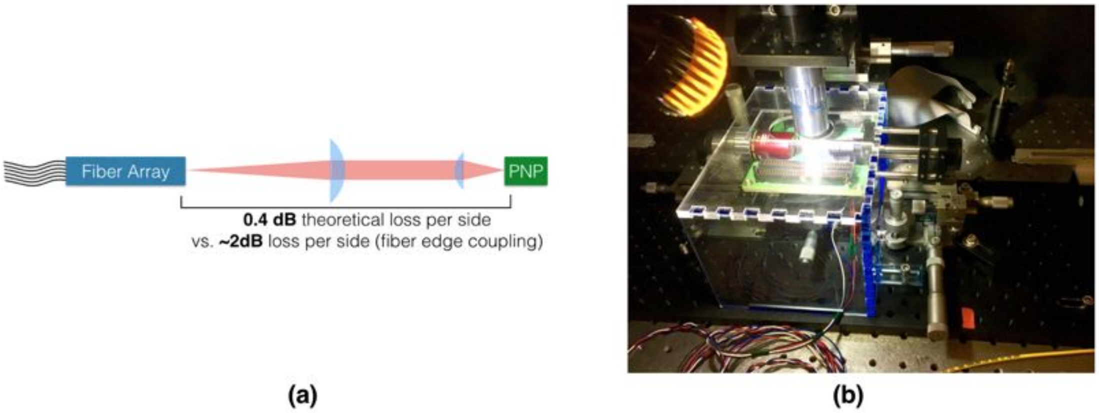

Fiber Array
PNP
0.4 dB theoretical loss per side
vs. ~2dB loss per side (fiber edge coupling)
(a)
(b)

Figure GM6. (a) Beam expansion system schematic for 5x demagnification of fiber array modes to one facet of the PNP chip. Using this lens system allows for coupling from a fiber array with a pitch and mode field diameter (MFD) of 127µm and 10µm, respectively, to the chip, having waveguide pitch and MFD of 25.4µm and 2µm, respectively. (b) Image of the setup, using an objective-lens system to couple to the left and a lens beam expansion system on the right.

Detection:
We are designing a homodyne detector array to realize shot-noise limited detection of the output modes. InGaAs P-I-N photodiodes obtained from Beijing SWT Optical Communication Technology constitute the detectors in this scheme.

Task 2: Resource-performance scaling in optical quantum processing

2.1 Resource scaling for an LOQC implementation in PIC-based linear optics

The goal of this task was to estimate resource scaling requirements for a useful all-optical quantum computing application. It is known that general-purpose quantum computers are in principle physically possible [2]. Recently, resource estimates for linear-optics quantum computing systems have been produced [3], though using non-optimal encoding. In fact, the optimal encoding depends critically on the application, which makes the problem statement poorly defined. To address a well-defined, specific problem, we proposed to instead analyze the recently proposed concept of all-optical quantum repeaters [4] that uses photon sources, linear optics, photon detectors and classical feedforward at each repeater node, but no quantum memories. We considered resource costs assuming realistic (though aggressive) device performance for the photon sources, detectors, and PIC-based mode transformations. This analysis quickly revealed that the original proposal would requirement astronomically many single photon sources and detectors per repeater node.

In theoretical work about to be published in Physical Review A, we showed that the quantum-secure key rate has the form $R(\eta) = D\eta^s$ bits per mode, where η is the end-to-end channel's transmissivity, and the constants D and s are functions of various device inefficiencies and the resource constraints, such as the number of available photon sources at each repeater node. Even with lossy devices, we show that it is possible to attain s<1, and in turn outperform the maximum key rate attainable without quantum repeaters, R_direct(η)=−log2(1−η)≈(1/ln2)η bits per mode for η≪1, beyond a certain total range L, where η~exp(−αL) in optical fiber. We also propose a suite of modifications to original all-optical repeater protocol[4], which lower the number of photon sources required to create photonic clusters at the repeaters so as to outperform R_direct(η), from ~10^{11} to ~10^6 photon sources per repeater node. We show that the optimum separation between repeater nodes is independent of the total range *L*, and is around 1.5 km for assumptions we make on various device losses.

This work is available on ArXiv[5] and accepted for publication in PRA. The detailed paper is also attached at the end of this report as an addendum.

2.2 Ballistic quantum computing with microclusters

It has been argued that BosonSampling -- sampling from the joint photon-number distribution at the output of a large multiport interferometer when multiple identical bosons are input into it -- is computationally hard for classical computers, but by-definition efficient on a quantum system [6], since the aforesaid (quantum) system samples efficiently from that distribution just by the virtue of being itself. A few practical uses of BosonSampling have been proposed in quantum simulation[7–9], but the scheme does not permit general purpose quantum computation -- or, so it is believed. On the other hand, it was recently shown that cluster states universal for quantum computation could be constructed by probabilisitically fusing 3-photon GHZ states, i.e., inputting 3-photon clusters at the input of a large interferometer, and without the use of feed-forward and switching, the output joint quantum state is universal for quantum computing [10], in the sense that no matter what is the actual shape of the instance of the sheet of entangled cluster that comes out of the linear optical interferometer, one can always detect a portion of it (some subset of modes), and use the measurement results to determine how to map any quantum algorithm instance into the cluster that lives on the remainder of the modes. This result by Terry Rudolph and collaborators, published in 2015, marked a major advance that suggested that building a linear-optical quantum computer may be far less challenging than previous estimates[3].

During the course of our SEQUOIA program, members of our team were able to make significant additional improvements on the efficiency of Ballistic cluster state generation. Most notably,

(1) we were able to establish, for the first time, a fundamental trade-off between the inline loss tolerance in the source-detection-efficiency product of each

source and every detector in the system, and the size k of the initial micro-cluster resource, so that universal quantum computing is possible, as shown in the figure below.

(2) Rudolph's work showed that as long as linear-optic Fusion operation at success probability > 62.5% is possible, one can do universal QC with k=3 (GHZ) micro-clusters as the starting resource. We reduced that achievability threshold to 59%. We also showed sufficient evidence that 54% is achievable (full proof is yet to be done), but showed that one has to have a success probability of Fusion greater than 1/(k-1), which for k = 3 microclusters is 50%. So, we have essentially closed the efficiency gap for Ballistic QC.

(3) In Rudolph's work that demonstrated the 62.5% achievable threshold for universal Ballistic QC, they used 3D clusters. We show it is possible with a 2D cluster, which reduces the device requirements tremendously. The reason this threshold was an important result is that Peter van Loock and others had shown in recent work that a Bell measurement (Fusion) at 75% success rate is possible using a linear-optics based scheme with single photons injected into the passive linear-optic circuit, if all the devices are lossless. Without those injected photons, the threshold can be no larger than 50%. Since 62.5% < 75%, Rudolph et al. had argued that Ballistic QC is possible as long as 3-photon GHZ states are available to start with. We have shown a particular 2D lattice, that a 74% success probability suffices the percolate the output cluster, and hence make universal Ballistic QC possible with this approach, and hence doable in principle with the aforesaid 75% boosted Fusion gate.

Remarkably, our work shows that experimentally near-term efficiencies may be tolerable for even moderately sized input-cluster states. Experimental progress towards systems that can produce such cluster states has been surprisingly fast: recently, it was demonstrated experimentally that photonic cluster states can be produced deterministically by photon scattering off a lambda-level system in semiconductor quantum emitters [11], thought the efficiency is still low and the system requires cryogenic cooling. As an alternative that may be operated at room temperature and fully lithographically controlled (as opposed to quantum dots), we have developed dielectric nonlinear sources of single photons and small entangled states[12]; see Section 3.3.

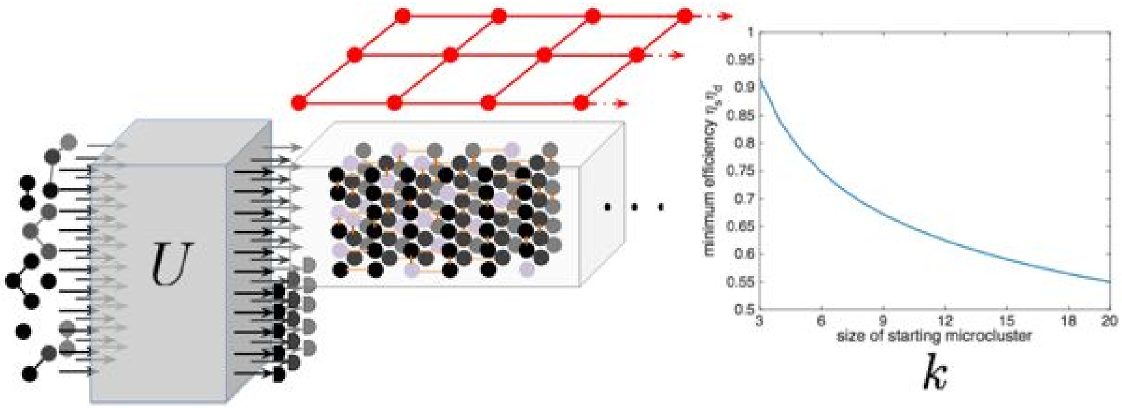

U
minimum efficiency $\eta_s\eta_d$
1
0.95
0.9
0.85
0.8
0.75
0.7
0.65
0.6
0.55
0.5
3
6
9
12
15
18
20
size of starting microcluster
k

Figure 2.2.1 Illustration of generation of scalable cluster state from micro-cluster input. k = 1 (Boson sampling), output cluster is disconnected: not a good enough resource for universal QC; k = 2 (Bell pair initial resource), output barely percolates if all efficiencies are 100% (no loss tolerance); k = 3 (3-photon GHZ is initial resource), then ballistic QC is possible; 3D-diamond (Rudolph et al.); λc = 62.5%; loss tolerance: ηsηd > 96.2%; (10,3)-b lattice (our method); λc = 54%; loss tolerance: ηsηd > 93.4%
Best possible lattice (converse proof / Bethe lattice); λc = 50%; max possible loss tolerance: 91.6%
Sources of >= 3-qubit microclusters needed if we want to avoid feed-forward, switching, and associated losses

Our resource analysis on ballistic linear optical quantum computing (LOQC) considered how to build a large continuous "sheet" of optical cluster state whose connectivity is pervasive and long-ranging enough to renormalize it (i.e., continuously carve out a logical cluster state from the random large spanning cluster that comes out of the interferometer) for universal quantum computing. The sheet of cluster state is prepared by preparing small k-photon cluster states (micro-clusters) and injecting them into a linear optical circuit. At the output, one detects a subset of the modes, and the remainder of the modes carry a resource universal for quantum computing regardless of the measurement results (the measurement results tell us how to use the giant entangled cluster on the remaining unmeasured modes to map any quantum algorithm to it). The special case of k=1 in the aforesaid way of looking at Ballistic quantum computing is exactly the Aaronson-Arkipov model of boson sampling. Our analysis revealed that a clear trade-off between the size of the input clusters k, and loss tolerance in the circuit, for the final sheet of cluster that comes out to be universal for quantum computing. In particular, by using new techniques from percolation theory, we showed that having N=3 size clusters as a starting resource is a must for loss-tolerant Ballistic LOQC using two-qubit fusion operations. This work establishes, for the first time, a clear trade-space between Aaronson-Arkipov boson sampling, i.e., k=1 (which does not allow universal quantum computing) to photonic cluster states that are universal for quantum computing (i.e., with GHZ states of size $k \geq 3$). k=2 (Bell states) happens to be a border-line case, where Ballistic LOQC is barely possible is all the linear-optic elements are 100% lossless, which of course is impractical.

This study told us that, for scalable LOQC, we need to consider scalable and efficient ways to directly produce $k \geq 3$ size photonic clusters (rather than first producing single photons and probabilistically stitching them together). This observation spurred us to investigate a structured means to directly generate 3-photon entangled GHZ state micro-clusters by exploiting six-wave mixing in a non-linear-optical waveguide. This idea, and associated calculations will be described in Task 3 below.

Task 3: Exploratory survey of key enabling technologies for scalable optical information processing

We have performed a thorough exploratory study surveying various key enabling technology components---including ones not being developed or pursued in Task 1 of this project for optical quantum information processing.

3.1 Wide-bandgap photonic integrated circuits for quantum information processing in the visible spectrum

How discussion so far on photonic integrated circuits has focused on the silicon on insulator (SOI) platform, which is technologically the most mature. However, this platform also has several important shortcomings: high-speed modulators are based on free carriage dispersion effects, which by their nature introduce some non-negligible loss and do not work well at cryogenic temperatures because of carrier freezeout; in addition, the circuit requires infrared photons above about 1.1 μ in wavelength come out which in turn requires superconducting detectors that add complications as compared to silicon avalanche photodetectors that could be used at shorter wavelengths. Therefore, we investigated here the possibility of an entirely different type of photonic integrated circuit based on the white bandgap III-nitrite material platform. This platform allows for electro-optic modulators based on chi-2 coefficient, which function well at low temperature and do not add free-carrier dispersion loss. Furthermore, wavelengths in the visible and potentially even the ultraviolet are compatible, allowing the use of room-temperature APDs. Without the need for superconducting detectors, the entire photonics platform can operate at room temperature. Moreover, the III-nitride platform allows for Kerr nonlinearities as well as chip-integrated light sources and detectors.

Specifically, we analyzed a PIC platform comprised of a crystalline AlxGa1-xN optical guiding layer on an AlN substrate for the ultraviolet to visible (UV-vis) wavelength range. An Al composition of x~0.65 provides a refractive index difference of ~ 0.1 and a small lattice mismatch (< 1%) that minimizes crystal dislocations at the AlGaN/AlN interface. This small refractive index difference is beneficial at shorter wavelengths to avoid extra-small waveguide dimensions. The platform enables compact waveguides and bends with high field confinement in the wavelength range from 700 nm down to 300 nm (and potentially lower) with waveguide cross-section dimensions comparable to those used for telecom PICs such as silicon and silicon nitride waveguides, allowing for well-established optical lithography. This platform can potentially enable cost-effective, manufacturable, monolithic UV-vis photonic integrated circuits. This study, which was a collaboration between BBN (Mohammad Soltani), MIT (Dirk Englund and Tomas Palacios) and the University of Massachusetts at Boston (Richard Soref), will appear in Optics Express.

3.2 Review of atom-like solid-state on-demand single photon sources

Single photon sources represent an essential resource in the applications considered in this program. However, experimentally, we are still some ways from an 'ideal' on-demand single- photon emitter. A wide range of promising material systems have been developed, and several have transitioned from proof-of- concept to engineering efforts with steadily improving performance. We reviewed recent progress in the race towards the ideal single-photon emitter required for a range of quantum information processing applications. We focused on solid-state systems including quantum dots, defects in solids, two-dimensional hosts and carbon nanotubes, as these are well positioned to benefit from recent breakthroughs in nanofabrication and materials growth techniques.

The central performance metrics of single photon sources are: source purity (lack of multi-photon emissions); photon indistinguishabilitiy (every photon emitted has the same mode shape); and efficiency (product of internal quantum efficiency and collection efficiency into a desired electromagnetic mode). Our review of recent works showed major deficiencies in the reporting of these source qualities. Reporting was most rigorous for InAs/GaAs self-assembled quantum dots, which were also the most advanced technologically, indistinguishability ~ 99%, efficiency ~ 75%, and photon purity g(2)(0)<1%.

A review article on these sources is published in Nature Photonics[13]

3.3 Proposal for on-demand single photon sources based on quantum feedback of a nonlinear dielectric cavity

As mentioned above, increased infidelity in the single photon states produced by sources sharply increases the resource overhead for quantum repeaters and ballistic quantum computing. Single photon sources based on atomic emitters have improved greatly over recent years -- for example, emission from InAs quantum dots can now achieve indistinguishability between consecutive photons in excess of 99% at an efficiency greater than 75% [13] -- but their performance still does not reach the desired >99% or so[5]. Moreover, single photon sources based on quantum emitters in solids typically have considerable inhomogenous distribution in emission. On the other hand, single photon sources based on heralded entangled pair generation can be very bright, operate at room temperature, have excellent photon indistinguishability. Moreover, many heralded sources based on nanophotonic circuits can be tuned perfectly into resonance[14,15]. A heralded single photon source relies on the information obtained from measurements of the device to predict its quantum state. It is normally implemented using a photon pair (signal and idler) source and a single photon detector that performs measurements on, e.g. the idler Hilbert space. The success probability of single photon generation can be increased by creating photons in multiple modes and multiplexing them into a single output mode. All the degrees of freedom of photons may be used as modes and multiplexing

both spatial, temporal, and frequency modes have been demonstrated. Spatial- and frequency multiplexing can produce modes in parallel from several individual sources or a frequency comb, respectively. Temporal multiplexing is a serial process where a single (a) source is triggered multiple times.

In our recent work, we considered temporal multiplexing, with the option to also use spectral multiplexing. The proposed architecture is shown in Fig. 1a, consisting of an ultrahigh Q microcavity with a χ (3) nonlinearity that allows signal and idler photons to be generated in pairs. The resonator is coupled to a switchable driving laser, a frequency- and photon number resolving detector (FPNRD), and an output channel via frequency selective tunable gates that control the coupling rates to the resonator.

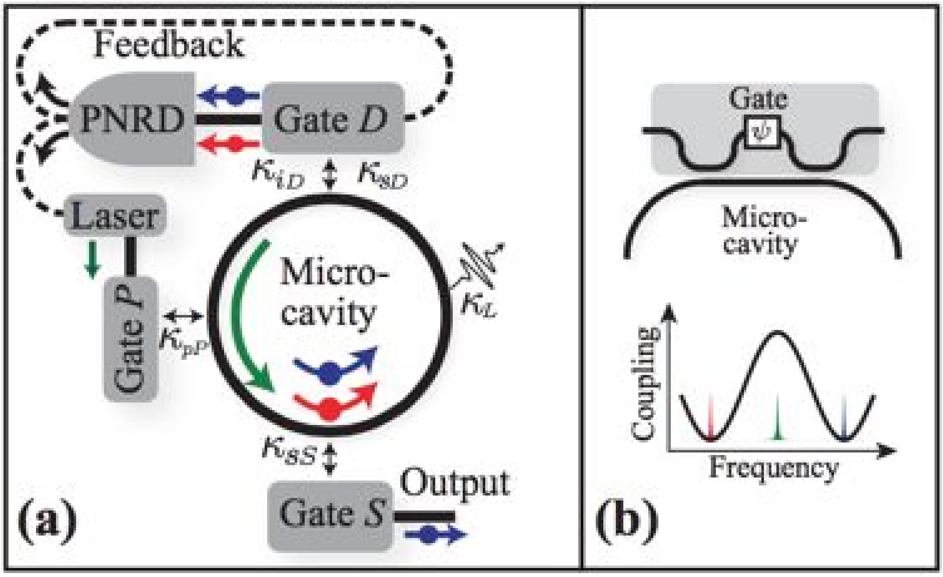


Fig. 3.3.1: (a) Proposed on-demand single photon source based on dynamic cavity storage. Subscripts i, p, s refer to idler, pump, and signal wavelength. Solid lines are optical waveguides, while dashed

lines represent electrical control signals. FP- NRD: Frequency- and photon number resolving detector. (b) Example of a gate implementation that has a large coupling for the pump frequency but is uncoupled for the signal and idler frequencies. This is achieved by matching the arm length difference of the MZI to the free spectral range of the micro cavity.

Figure 3.3.2 plots the single-photon fidelity Fth (%) against the probability of a heralding event in a given clock cycle, for a range of detector efficiencies η. This device uses temporal heralding in a single ring only. With a heralding probability of even just P(success)=30% (corresponding to η=0.99 and Fth=0.98) , spectral multiplexing over 15 multiple sources increases the probability of heralding at least one event increases to $1-(1-0.3)^{15}>99.5\%$. Thus, such a source could produce single photons of sufficient efficiency and fidelity.

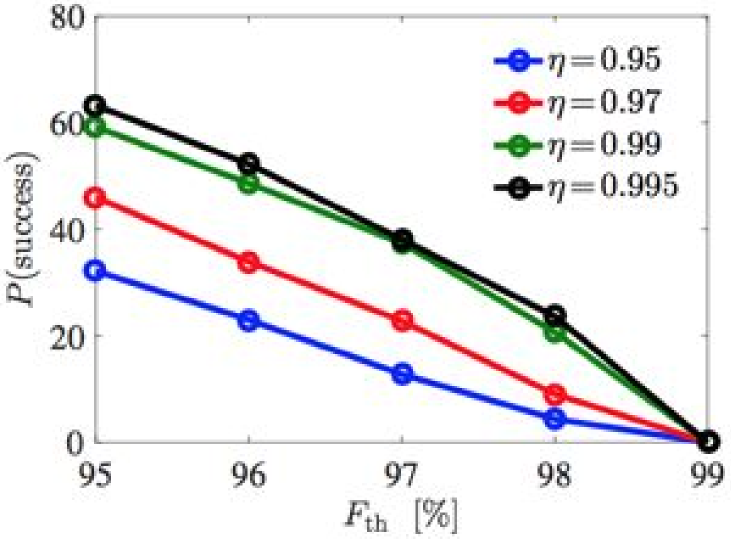
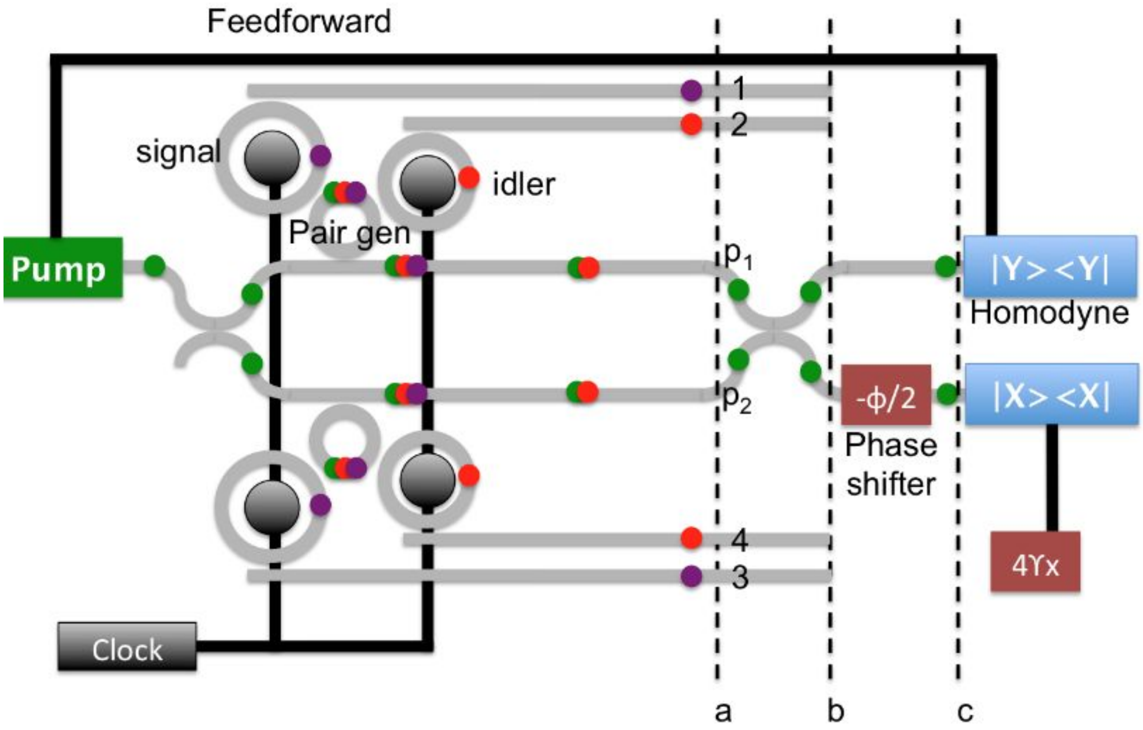


Figure 3.3.2: Fidelity vs heralding trade-off.

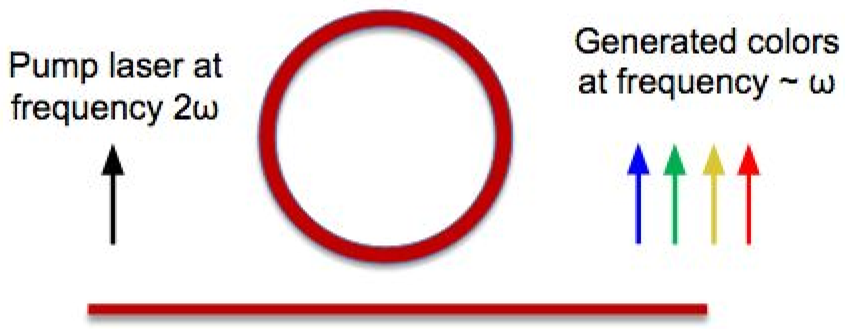
3.4 On-demand GHZ source based on QND and dynamic cavity control (manuscript in preparation)

As mentioned above, 3-photon GHZ states form a minimal resource for loss-tolerant production of cluster states for ballistic quantum computing. However, no efficient 3-photon GHZ state source exists today. To this end, we have extended the concept of the on-demand single photon source by cavity feedback (Section 3.3) to produce 3-photon GHZ states. The central idea is to monitor the cavity photon population using quantum nondemolition measurements of the cavity modes, using cross-Kerr nonlinear interactions with the probe beam and homodyne detection, as shown in the figure below.



3.5 3-photon GHZ source based on 6-wave mixing (manuscript in preparation)

Another way to produce 3-photon GHZ states is by 6-wave mixing, as illustrated below. We are currently investigating this method.



3.6 Quantum Logic with Interacting Bosons in 1D

We also developed a scheme[16] for implementing high-fidelity quantum logic gates using the quantum walk of a few interacting bosons on a one-dimensional lattice. The gate operation is carried out by a single compact lattice described by a one-dimensional Bose-Hubbard model with only nearest-neighbor hopping and on-site interactions. We find high-fidelity deterministic logic operations for a gate set (including the CNOT gate) that is universal for quantum information processing. We analyzed the applicability of this scheme in light of recent developments in controlling and monitoring cold-atoms in optical lattices, as well as an implementation with realistic nonlinear quantum photonic devices. This work is currently under review. Figure 3.6.1 shows the evolution of a two dual-rail photon states (control and signal) undergoing a controlled logic gate, assuming a two-photon interaction (such as mediated by the Kerr nonlinearity or an atomic nonlinearity). For details, see Ref. [16]

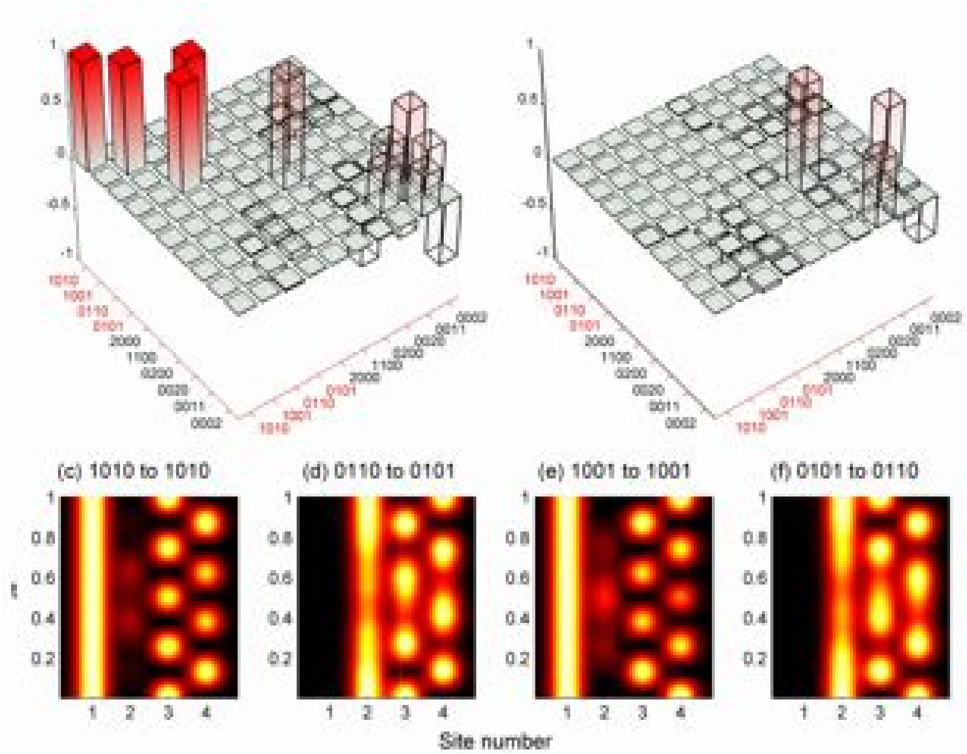


Figure 3.6.1 An implementation of the controlled NOT (CNOT) gate (a) The real part and (b) the imaginary part of the two-particle unitary transform, U. The CNOT gate operation corresponds to the sub-matrix of the logic states, shown in solid-color bars and marked with red axis labels. Plots (c)-(f) show the position (in terms of the lattice sites, 1-4) of the particle density as a function of time, t, revealing the operation principle of the gate on each logical state (|00>, |10>, |01>, and |11> respectively). One observes that the target qubit (in sites 3 & 4) performs Rabi-oscillations that are perturbed by the state of the control qubit (in sites 1 & 2) — the target qubit performs one fewer Rabi-flip if the control qubit is in the |1> state.

3.7 Limitations of two-level emitters as non-linearities in passive two-photon controlled phase gates

Two-level atomic systems in cavities are often cited as one possible mechanism for producing two-photon phase gates (or other two-photon logic gates). We investigated various architectures and found that it is not possible to reach unity fidelity for such gates for a time-invariant cavity.

Using a "dual Hong-Ou-Mandel" geometry shown in Figure 3.7.1, we were able to ensure that the incoming and existing photon states are in the dual-rail logic representation.

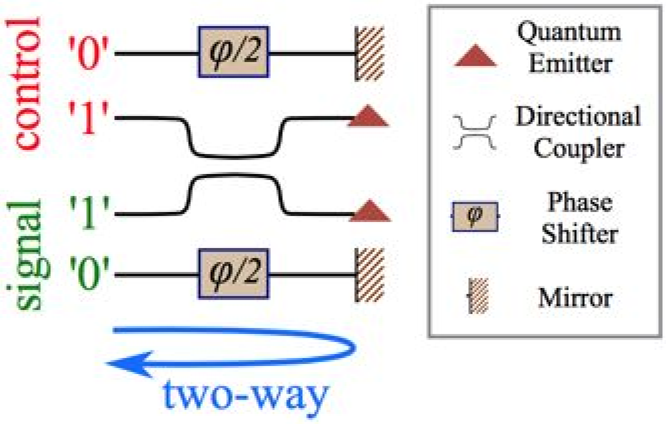


Figure 3.7.1 Schematic of two-photon phase gate.

We analyzed such gates under the action of finite-duration photon wave packets for signal and control photons. The two-photon gate fidelity is plotted in Figure 3.7.2, where v_g is the group velocity in the waveguides (for signal and control photons) and Γ the emitter decay rate into waveguide modes.

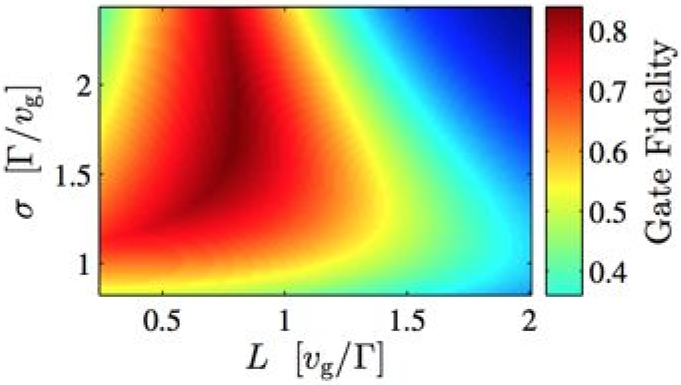


Figure 3.7.2 Gate fidelity simulation results.

We plan to expand this analysis to time-dependent waveguide-cavity coupling, which promises to actually allow near-unity gate fidelity.

4. Future Directions in Optical Quantum Computing and Networking

This seedling program has improved devices and developed theoretical protocols that greatly lowered the resource requirements of linear optics quantum computing and all-optical quantum repeaters. This section considers promising future directions.

4.1 Photonic nanocavity design to achieve room-temperature single-photon strong coupling with dielectric materials

We developed a photonic crystal nanocavity design with arbitrarily small mode volume(Veff), which allows nonlinear optical response at the single-photon level. The design relies on enhancement based on two electric field boundary conditions. These methods can be concatenated to further reduce Veff. Depending on the termination, both dielectric and air cavity can be designed for a target application. We illustrate the nanocavity concept in a silicon-air nanobeam at 1550 nm that reaches an ultrasmall volume Veff~$2*10^{-4}(\lambda/n)^3$. With a suitable chi-3 medium, this cavity allows single-photon nonlinearity -- even at room temperature.

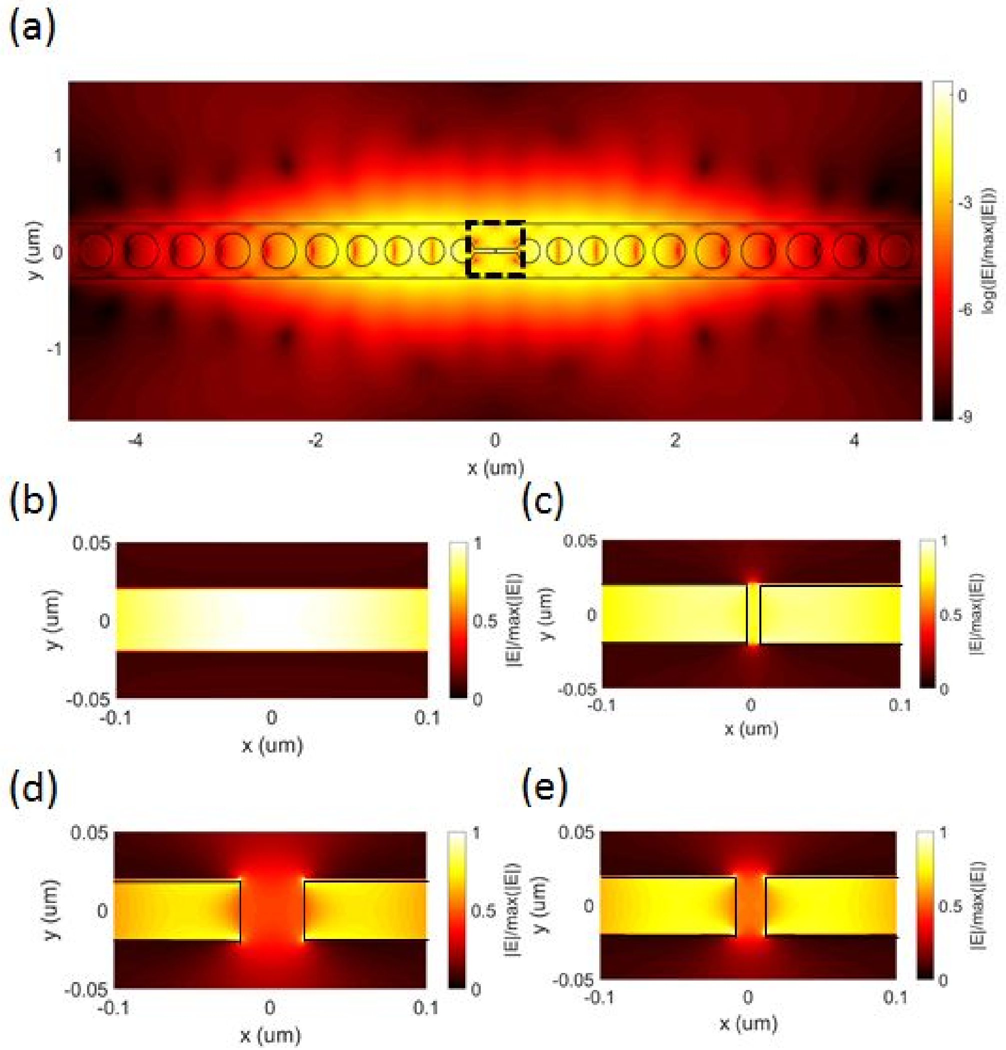


Fig 4.1.1 (a) Geometry of base structure (b)~(e) Electric field distribution. (inset) Electric energy density. (b) Type 1 enhancement (slot cavity). (c) Type 2 enhancement with narrow bridge (5nm). (d) Wide bridge (40nm). (e) intermediate size bridge (20nm).

Optical nanocavities with small mode volume (V_{eff}) and high quality factor (Q) can greatly increase the light-matter interaction and have a wide range of application including nanocavity lasers, cavity quantum electrodynamics (cQED), and nonlinear optics. Photonic crystal (PhC) cavities with an air slot can achieve exceptionally small V_{eff} on the order of $0.01\lambda^3$, where λ is the free-space wavelength[17,18]. This cavity relied on enhancement through a boundary condition on normal electric displacement. We demonstrated further reduction of V_{eff} using the second boundary condition on parallel electric field.

Furthermore, concatenation of both enhancement enables arbitrarily small V_{eff}, limited only by practical considerations such as fabrication resolution. The extreme field confinement of this cavity design opens new possibilities in nonlinear optics; in particular, such cavity designs can enable Kerr-nonlinear optical phenomena at the single photon level.

Typical photonic crystal cavity obtains field confinement through interference that limits the size of confinement as half wavelength ($V_{eff} \sim (\lambda/2n)^3$): diffraction limit. However, V_{eff}, which is local in the sense that it is determined by field at one position (maximum field), is not strictly limited by the diffraction limit if field confinement does not come from interference: strong inhomogeneity of medium. Mode volume reduction beyond the diffraction limit has been studied with slot cavities by Lipson and coworkers [19,20]. In a slot cavity, field in low index region is enhanced through boundary condition on electric displacement:

$$\varepsilon_h E_h = D_{h\perp} = D_{l\perp} = \varepsilon_l E_l \ldots\text{(4.1.2)}$$

$$E_l = \tfrac{\varepsilon_h}{\varepsilon_l} E_h \ldots\text{(4.1.3)}$$

where subscript l and h mean low and high index respectively, and $\perp$ means normal component of field with respect to boundary. Maximum electric energy density is increased by a factor of:

$$\frac{W_{e1}}{W_{e0}} = \frac{\varepsilon_l |E_l|^2}{\varepsilon_h |E_h|^2} = \frac{\varepsilon_h}{\varepsilon_l} \ldots\text{(4.1.4)}$$

If we assume that a slot is narrow that the numerator of (1) is not changed by a slot, then V_{eff} is reduced by a factor of $\varepsilon_h/\varepsilon_l$. For a silicon-air nanobeam cavity, this enhancement is $\varepsilon_h/\varepsilon_l \sim 13.9$ and mode volume$\sim 0.01\lambda^3$ was achieved [17,18]. Field enhancement through normal electric displacement continuity (Type 1 enhancement) is advantageous in that it is inherently wavelength independent endowing more tolerance to errors occured from simulation and fabrication. However, since a cavity has high electric field in low index region (air cavity), there has been limited applications.

Here, we propose a method to further reduce V_{eff} with parallel electric field continuity across a boundary (Type 2 enhancement). More specifically, this is achieved by a high index bridge across a slot (Fig. 1(a)). Parallel electric field across the boundary is given by (5):

$$E_{h\|} = E_{l\|} \ldots(4.1.5)$$

Through Type 2 enhancement, large electric field in low index region (slot) is transferred into high index region (bridge). As a result, the bridge has the largest electric energy density; cavity is a dielectric cavity. This cavity is useful when one needs light-matter interaction in high index material. Maximum electric energy density enhancement is given by (4.1.6):

$$\frac{W_{e2}}{W_{e1}} = \frac{\varepsilon_h |E_h|^2}{\varepsilon_l |E_l|^2} = \frac{\varepsilon_h}{\varepsilon_l} \ldots(4.1.6)$$

In the same logic with the Type 1, if a bridge is narrow enough that adding a bridge out of a slot does not change the numerator of (1), then $V_{eff}$is reduced by a factor of $\varepsilon_h/\varepsilon_l$.

To demonstrate our assertion, 3D finite-difference time-domain (FDTD) simulation was conducted on the nanobeam cavities depicted in figure 1(a) with variations on the dashed box. Simulated V_{eff} is $9.48 \times 10^{-21}(2.54 \times 10^{-3}(\lambda)^3)$, which is ~10 times smaller than the V_{eff} of slot cavity $(9.47 \times 10^{-20},\ 2.51 \times 10^{-2}(\lambda)^3)$. This enhancement is slightly smaller than $\varepsilon_h/\varepsilon_l = 12.09$ because of the finite size of bridge and electric field components perpendicular to the boundary. "Enhancement by boundary condition" only happens when one boundary condition is dominant over the other. In a slot cavity (figure 4.1.2(b)), lateral boundary between low index and high index should be dominant over the vertical boundary between slot and holes. For the field in the bridge to be forced same as the field in slot, vertical boundary between high index region and low index region should be dominant over the lateral boundary between the bridge and high index slab. Figure 4.1.2(d) and 4.1.2(e) illustrate simulation results when the previously stated requirement is not satisfied. For a wide or intermediate width bridge case, field in the bridge is not same with that in the slot because effects from boundary between bridge and slab is not negligible. However, there is still enhancement.

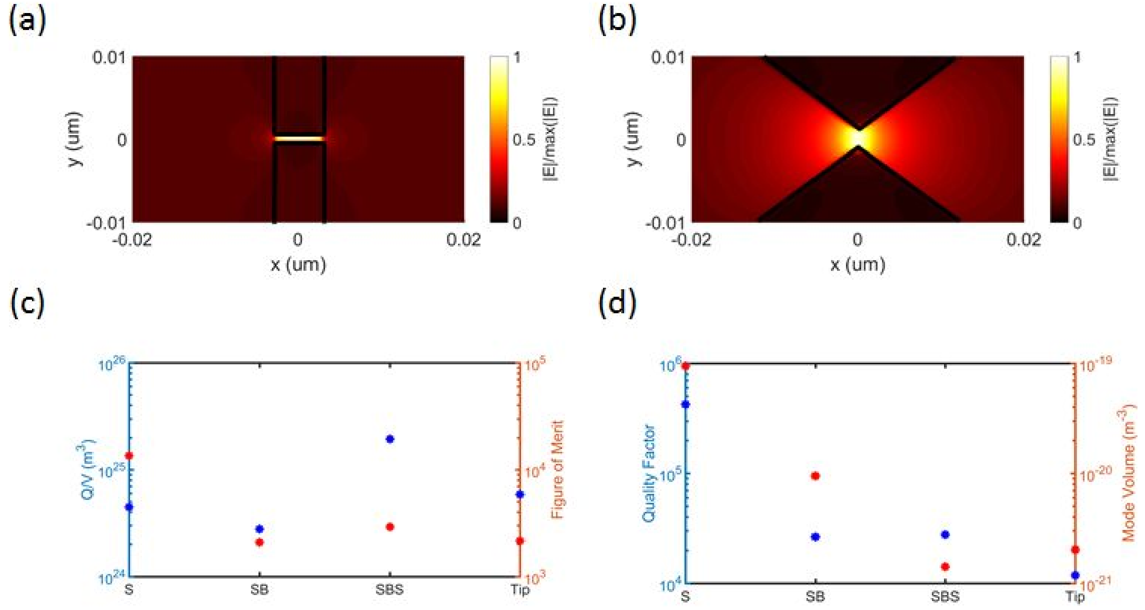


Fig 4.1.2. Electric field distribution. (a) 2nd level slot (SBS) (b) Tip shape as a limiting case of concatenation. Here, we show air cavity limit of a tip. (c) Quality factors and mode volume in each level. (d) Two figure of merit: Q/V as a general criteria and QV_M/V_{eff}^2 for strong coupling.

We furthermore find that the extreme light confinement allows us to reach the strong coupling regime: a single photon injected into the cavity produces a sufficient index shift (by Kerr nonlinearity) that the cavity frequency shifts by more than one linewidth, assuming a Q factor > 100,000 and materials inside the cavity gap such as Graphene ($0.5 * 10^{-13} m^2/V^2$ Zhang et al. 2012), Indium Tin oxide ($0.5 * 10^{-16} m^2/V^2$ [21]), and J-aggregate ($0.5 * 10^{-13} m^2/V^2$ Zhuravlev et al. 1992).

4.2 All-Optical Ising Machine

Devices that can solve the Ising model via quantum annealing, a restricted class of adiabatic quantum computers have recently gained popularity, since the Ising model can encode many interesting NP hard optimization problems. It is however not yet clear if quantum annealing provides speed up in terms of how the number of computational steps scale as the size of the problem grows as compared to the best classical algorithms. All quantum annealing architectures realized to date employ `matter' qubits, such as superconducting, NMR and Bose-Einstein condensates. Even in the absence of a computational complexity advantage, an all-optical quantum annealer could be very attractive both due to its ability to gain a large constant-factor speedup, as well as achieve a potentially large power saving, over conventional electronic-computing solutions. We designed an all-optical realization of quantum annealing and an explicit integrated photonic architecture for its implementation. The proposed architecture employs an array of spectral-dual-rail encoded optical qubits in a single pair of coupled non-linear cavities, and dynamically-tunable linear-optic and cross-phase interactions across pairs of qubits, with very small yet tunable non-linear phases. Our calculations show that the maximum nonlinearities required in the protocol are of the order of 10^{-4}. Such nonlinearities would be easily achievable using the fractal cavities described in the previous section.

Program Journal Publications

1. Yoav Lahini, Gregory R. Steinbrecher, Adam D. Bookatz, Dirk Englund, ''High-fidelity Quantum Logic Gates with Interacting Bosons on a 1D Lattice,'' arXiv:1501.04349 (2015)
2. Mihir Pant, Hari Krovi, Dirk Englund, Saikat Guha, ''Rate-distance tradeoff and resource costs for all-optical quantum repeaters,'' arXiv:1603.01353 (2016)
3. Anders Nysteen, Dara P. S. McCutcheon, Mikkel Heuck, Jesper Mørk, and Dirk R. Englund, ''Limitations of two-level emitters as non-linearities in passive two-photon controlled phase gates,'' under review (2016)
4. Mikkel Heuck, Mihir Pant, and Dirk englund, ''Temporally Multiplexed Single Photon Source using Photon Addition and Subtraction with Quantum Feedback Control,'' submitted (2016)
5. Hyongrak Choi and Dirk Englund, ''Self-similar nanocavity design with arbitrarily small mode volume for single-photon nonlinearity,'' to be submitted (2016)

Program Conference Presentations

- D. Englund et al, ''Towards scalable networks of solid state quantum memories in a photonic integrated circuit,,'' Second SIPQNP workshop, Raytheon BBN, Cambridge, MA. (3/13/2015)
- D. Englund et al, ''Semiconductor Quantum Technologies for Information Processing and Sensing,,'' University of Calgary Institute for Quantum Science and Technology Colloquium, Calgary, Canada. (4/16/2015)
- D. Englund et al, ''Quantum Information Processing Using Active Silicon Photonic Integrated Circuits,,'' Workshop on Multi-Photon Interferometry, University of Science and Technology, Shanghai, China. (5/7/2015)

- D. Englund et al, ''Semiconductor Quantum Technologies for Information Processing and Sensing,,'' Canadian Institute for Advanced Research - Quantum Information Science Program Meeting, Toronto, Canada. (6/5/2015)
- Jacob Mower, Nicholas C. Harris, Gregory R. Steinbrecher, Faraz Najafi, Yoav Lahini, Tom Baehr-Jones, Michael Hochberg, Karl K. Berggren, and Dirk Englund, ''Quantum Information Processing Using Active Silicon Photonic Integrated Circuits,'' CLEO/Europe-EQEC 2015, Munich, Germany (6/22/2015)
- D. Englund et al, ''Quantum Photonic Processors,'' , Majorca at MIT, MIT, Cambridge, MA (7/28/2015)
- D. Englund et al, ''Towards scalable networks of solid state quantum memories in a photonic integrated circuit,'' , SPIE (8/28/2015)
- D. Englund et al, ''Progress Towards Scalable Entanglement of Spin Qubits in Photonic Integrated Circuits,'' , GeneExpression Systems & Appasani Research Conferences - Physical Sciences Symposia, Cambridge, MA (9/22/2015)
- D. Englund et al, ''Quantum information processing using active silicon photonics integrated circuits,'' , RIEC-RLE Meeting, Tohoku University, Sendai, Japan (10/27/2015)
- D. Englund et al, ''Semiconductor Quantum Technologies for Information Processing and Sensing,'' , ASD(R&E) Basic Research Forum, Arlington, VA (12/10/2015)
- Mihir Pant, Hari Krovi, Dirk Englund and Saikat Guha, ''Rate-distance tradeoff and resource costs for all-optical quantum repeaters,'' SIPQNP 2016 (2016)
- Mihir Pant, Hari Krovi, Dirk Englund and Saikat Guha, ''Rate-distance Tradeoff and Resource Costs for All-Optical Quantum Repeaters,'' QCrypt 2016 (2016)
- Di Zhu, Hyeongrak Choi, Tsung-Ju Lu, Qingyuan Zhao, Andrew Dane, Faraz Najafi, Dirk R Englund, Karl Berggren, “Superconducting Nanowire Single-Photon Detector on Aluminum Nitride,” CLEO 2016 (6/5/2016)
- Karl Berggren et al, “Superconducting Nanowire Single-Photon Detectors and Nanowire-Based Superconducting On-Chip Electronics,” CLEO 2016 (6/5/2016)

Patents

References

[1] S. Guha, Phys. Rev. Lett. **106**, (2011).
[2] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).
[3] Y. Li, P. C. Humphreys, G. J. Mendoza, and S. C. Benjamin, Phys. Rev. X **5**, (2015).
[4] K. Azuma, K. Tamaki, and H.-K. Lo, Nat. Commun. **6**, 6787 (2015).
[5] M. Pant, H. Krovi, D. Englund, and S. Guha, arXiv [quant-Ph] (2016).
[6] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, USA, 2011), pp. 333–342.
[7] B. Peropadre, J. R. McClean, and A. Aspuru-Guzik, Nature (2015).
[8] D. González Olivares, B. Peropadre, A. Aspuru-Guzik, and J. J. García-Ripoll, Phys. Rev. A **94**, (2016).
[9] K. R. Motes, J. P. Olson, E. J. Rabeaux, J. P. Dowling, S. J. Olson, and P. P. Rohde, Phys. Rev. Lett. **114**, 170802 (2015).
[10] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **115**, 020502 (2015).
[11] I. Schwartz, D. Cogan, E. R. Schmidgall, Y. Don, L. Gantz, O. Kenneth, N. H. Lindner, and D. Gershoni, Science (2016).
[12] M. Heuck, M. Pant, and D. R. Englund, in *Conference on Lasers and Electro-Optics* (OSA, Washington, D.C., n.d.), p. FTu4C.7.
[13] I. Aharonovich, D. Englund, and M. Toth, Nat. Photonics **10**, 631 (2016).
[14] N. C. Harris, D. Grassani, A. Simbula, M. Pant, M. Galli, T. Baehr-Jones, M. Hochberg, D. Englund, D. Bajoni, and C. Galland, Phys. Rev. X **4**, 041047 (2014).
[15] N. C. Harris, D. Bunandar, M. Pant, G. R. Steinbrecher, J. Mower, M. Prabhu, T. Baehr-Jones, M. Hochberg, and D. Englund, Nanophotonics **5**, (n.d.).
[16] Y. Lahini, G. R. Steinbrecher, A. D. Bookatz, and D. Englund, arXiv [quant-Ph] (2015).
[17] J. T. Robinson, C. Manolatou, L. Chen, and M. Lipson, Phys. Rev. Lett. **95**, 143901 (2005).
[18] P. Seidler, K. Lister, U. Drechsler, J. Hofrichter, and T. Stöferle, Opt. Express **21**, 32468 (2013).
[19] V. R. Almeida, Q. Xu, C. A. Barrios, and M. Lipson, Opt. Lett. **29**, 1209 (2004).
[20] J. T. Robinson, M. Christina, C. Long, and L. Michal, Phys. Rev. Lett. **95**, (2005).
[21] M. Z. Alam, I. De Leon, and R. W. Boyd, Science **352**, 795 (2016).

Rate-distance tradeoff and resource costs for all-optical quantum repeaters

Mihir Pant,[1, 2, *] Hari Krovi,[2] Dirk Englund,[1] and Saikat Guha[2]

[1] *Dept. of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139, USA*
[2] *Quantum Information Processing group, Raytheon BBN Technologies,*
10 Moulton Street, Cambridge, MA 02138, USA

We present a resource-performance tradeoff of an all-optical quantum repeater that uses photon sources, linear optics, photon detectors and classical feedforward at each repeater node, but no quantum memories. We show that the quantum-secure key rate has the form $R(\eta) = D\eta^s$ bits per mode, where η is the end-to-end channel's transmissivity, and the constants D and s are functions of various device inefficiencies and the resource constraint, such as the number of available photon sources at each repeater node. Even with lossy devices, we show that it is possible to attain $s < 1$, and in turn outperform the maximum key rate attainable without quantum repeaters, $R_{\text{direct}}(\eta) = -\log_2(1-\eta) \approx (1/\ln 2)\eta$ bits per mode for $\eta \ll 1$, beyond a certain total range L, where $\eta \sim e^{-\alpha L}$ in optical fiber. We also propose a suite of modifications to a recently-proposed all-optical repeater protocol that ours builds upon, which lower the number of photon sources required to create photonic clusters at the repeaters so as to outperform $R_{\text{direct}}(\eta)$, from $\sim 10^{11}$ to $\sim 10^6$ photon sources per repeater node. We show that the optimum separation between repeater nodes is independent of the total range L, and is around 1.5 km for assumptions we make on various device losses.

PACS numbers: 42.50.Ex, 03.67.Dd, 03.67.Lx, 42.50.Dv

I. INTRODUCTION

Quantum key distribution (QKD) enables two distant authenticated parties Alice and Bob, connected via a quantum (e.g., optical) channel, to generate information-theoretically secure shared secret bits. No knowledge of the channel conditions (noise model, or any channel estimate) is required a priori to ensure security. However, the shared secret is generated at a rate commensurate with the worst-case adversary physically consistent with the channel conditions actually presented to Alice and Bob. The reason is that all the perceived channel imperfections (absolutely anything that causes the channel map to deviate from a noiseless identity transformation) is attributed to the actions of the most powerful adversary allowed by physics—even though some (or all) of that deviation of the channel from an identity map may actually stem from non-adversarial sources, such as losses due to free-space diffraction, fiber loss, detection inefficiency, thermal noise from blackbody at the operating temperature and wavelength, and detector noise. An important consequence of this assumption is that all the signal power transmitted by Alice that is not collected by Bob is made available coherently to the eavesdropper, Eve. This model for Eve is the intuition behind why the secret key rate for a direct-transmission based QKD protocol must decrease linearly with η, the Alice-Bob power transmissivity, in the $\eta \ll 1$ regime [1, 2]. For any direct-transmission protocol over the pure-loss optical channel of transmissivity η, and assuming unlimited authenticated two-way public classical communication, it was recently shown that the key rate cannot exceed $-\log_2(1-\eta)$ bits per mode [2], which is $\approx 1.44\eta$ for $\eta \ll 1$. For a pure-loss channel, the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) upper bound improves over the Takeoka-Guha-Wilde (TGW) bound [1] by a factor of 2 in the $\eta \ll 1$ regime. The TGW bound is an upper bound on the secret-key agreement capacity with unlimited two-way classical communication $P_2(\mathcal{N})$, applicable to a general quantum channel $\mathcal{N}$. For the pure-loss channel $\mathcal{N}_\eta$, the PLOB bound coincides with the best-known achievable rate [3], thus establishing $P_2(\mathcal{N}_\eta) = -\log_2(1-\eta)$ bits per mode. From hereon, we denote by $R_{\text{direct}}(\eta) \equiv -\log_2(1-\eta)$ the maximum bits-per-mode secret key rate achievable by any direct-transmission QKD protocol, i.e., without the use of quantum repeaters. The bits/s rate of a QKD protocol's implementation is obtained by multiplying the bits/mode rate by the spatio-temporal-polarization bandwidth (modes/s), which is governed by the channel geometry, and the transmitter and detector bandwidth. Since loss increases exponentially with distance L in optical fiber (i.e., $\eta = e^{-\alpha L}$), for $\eta \ll 1$, the key rate generated by any direct-transmission QKD protocol must decay exponentially with the range L. Expressed as a function of L, $R_{\text{direct}}(L) = -\log_2(1-e^{-\alpha L})$ bits/mode, which is $\approx 1.44e^{-\alpha L}$ bits/mode, for L large.

Quantum repeaters, proposed in [4], are devices which when inserted along the length of the optical channel, can help generate shared secret at a rate that surpasses $R_{\text{direct}}(\eta)$ at any value of Alice-to-Bob channel transmissivity η [2]. Quantum repeaters need not be trusted or physically secured in order to ensure the security of the keys generated. If n quantum repeaters are inserted along the length of the channel connecting the communicating parties Alice and Bob, and if there are absolutely no physical constraints placed on the repeater nodes (i.e., the repeaters are assumed to be

[*] mpant@mit.edu

lossless, error-corrected, general purpose quantum computers), then the maximum key rate achievable by Alice and Bob is given by $-\log_2(1-\eta_{\min})$ bits/mode, where $\eta_{\min} \equiv \min(\eta_1, \eta_2, \ldots, \eta_{n+1})$, with $\eta = \eta_1 \ldots \eta_{n+1}$, is the transmissivity of the lossiest link between successive repeater nodes [5] (see [6] for a different upper bound based on squashed entanglement [1]). Given n ideal repeater nodes, their optimal placement is to lay them equally-spaced, in which case, the maximum achievable rate is $-\log_2(1-\eta^{1/(n+1)})$ bits/mode. As $n \to \infty$, the rate is unbounded. However, assuming repeaters to be lossless error-corrected quantum computers is not practical. A more practically relevant question to ask is if the repeater nodes have finite resources with lossy and imperfect components (where 'resources' may be different physical entities depending upon the type of quantum repeater and the protocol employed), then what rate can Alice and Bob achieve, and more importantly what would it take to build repeater nodes so as to be able to significantly outperform $R_{\text{direct}}(\eta) = -\log_2(1-\eta)$ bits/mode. This is the topic addressed in this paper, for repeaters that are built solely using photonic components—single-photon sources, detectors, electro-optic feedforward, but no matter-based quantum memories. As we will see later in this paper, that given physical constraints on a repeater node, placing more repeaters (higher n) between Alice and Bob may not always improve the rate, i.e., depending upon the total distance L (or equivalently, the transmissivity η) between Alice and Bob, and given the physical device constraints in a repeater node, there may be an optimal number $n^*(\eta)$ of nodes, which achieves the highest end-to-end rate.

Traditional quantum repeaters work in the framework of entanglement-based QKD. At the end of the transmission phase of an entanglement-based QKD protocol, Alice and Bob share (noisy, or imperfect) entangled pairs (e.g., of photons or matter-based stationary qubits) which could have been tampered with, or which could have deteriorated due to channel loss and noise. At that point, if the end goal of Alice and Bob is to generate shared entanglement (for use in some quantum protocol that consumes shared entanglement, such as teleporation [7] or dense coding [8]), they would perform *entanglement distillation* to sieve out a small number of clean maximally entangled Bell pairs by performing local operations and classical communications (LOCC). If the end goal of Alice and Bob is to generate shared secret (a strictly less demanding goal than generating shared entanglement), they directly measure the noisy shared entangled pairs, and perform (classical) error correction and privacy amplification on their correlated measurement results over an authenticated public channel to distill a quantum-secure shared secret key.

Several different genres of repeater protocols have been proposed [9]. The two primary ingredients in any of the traditional repeater architectures are: (1) some form of a quantum memory, and (2) the ability to perform a certain restricted class of quantum logic, i.e., gates and measurements on the flying (photonic) qubits as well as the static (memory) qubits. In the most basic repeater protocol, the restricted quantum operation required is Bell state measurement (BSM) on pairs of qubits. A BSM on qubit b and qubit c converts two independent Bell pairs $|\Psi\rangle^{ab}$ and $|\Psi\rangle^{cd}$ into one Bell pair $|\Psi\rangle^{ad}$, upto local single qubit operations, a process known as *entanglement swapping.*

A. Quantum repeaters based on mode multiplexing and Bell state measurements

In the following discussion, we will focus on a class of quantum repeaters that rely solely on probabilistic BSMs, quantum memories, and multiplexing, i.e., the ability to 'switch' qubits across (spatial, spectral, or temporal) modes. The essence of such a repeater protocol was developed by Sinclair *et al.* [10], which employed spectral multiplexing in multimode quantum memories across m parallel (spectral) channels, and entanglement swapping using linear optics and single photon detectors (the success probability of which can at most be 50%). Guha *et al.* analyzed the secret key rates achievable by the above protocol, with a fixed m (memory size) and found that even when photon loss is the only source of noise, the achievable key rate is of the form $R(\eta) = D\eta^s$ bits/mode, where D, and $s < 1$ are constants that are functions of various losses in the system (e.g., detection efficiencies, coupling losses, memory loading and readout efficiencies, and BSM failure probability) [11]. Since the exponent of η, i.e., s is strictly less than 1, the key rate must beat $R_{\text{direct}}(\eta)$ (which scales as: $\propto \eta$ for $\eta \ll 1$) beyond a certain minimum distance determined by the actual values of the system's loss parameters, which is around a couple of hundred kilometers for reasonable estimates of the losses [11]. Since $\eta = e^{-\alpha L}$ in fiber, the rate achieved by this repeater protocol for a fixed memory size, $R(L) = De^{-s\alpha L}$ still scales exponentially with the range L, albeit with a smaller exponent compared to the best possible rate without any repeater, which could turn into a huge absolute improvement in the end-to-end secret key rate [11].

Azuma *et al.* recently proposed an all-photonic variant of this protocol in which they substituted matter based quantum memories with optical cluster states [12], based on a proposal by Varnava *et al.* to mimic a quantum memory (i.e., protect against photon losses) by appending each physical photonic qubit by an entangled 'tree cluster' state [13]. As long as the losses incurred by each photon (i.e., photons being protected as well as the additional photons in the trees added for loss protection) is less than 3 dB, the effective loss of the logical qubit can be made to approach zero, by increasing the size of the tree cluster, i.e., the number of photons in the logical qubit [14]. Thus, Azuma *et al.*'s proposal showed the theoretical feasibility of a quantum repeater architecture (i.e., one that can beat the scaling of direct-transmission

QKD) using only flying qubits, with the repeater *nodes* being equipped only with single photon sources, passive linear-optical circuits (beamsplitters and phase shifters), single photon detectors, and classical feedforward.

Azuma *et al.*'s result marked a promising conceptual leap towards all-optical quantum repeaters. However, important unanswered questions remained, including the achievable secure key generation rate and how it scales with distance (or loss), as well as the physical resource requirements: e.g., the number of photon sources and detectors at the repeater nodes. As an example, a calculation in their paper shows that at a range of $L = 5000$ km, an entanglement-generation rate of 69 kHz is achievable in a fiber based linear optic system with 100 kHz repetition rate, 150 ns feed forward time and a source-detector efficiency product of 95% whereas sharing a single entangled photon pair via a direct transmission scheme with the same parameters would require 10^{81} years. The level of error protection required to achieve the aforesaid repeater performance at $L = 5000$ km would require one to build entangled clusters of $\sim 10^4$ photons at the 100 kHz clock rate at each repeater node. Building such a cluster using linear optics and feed-forward [15, 16] would require around 10^{24} single photon sources at each repeater node. Furthermore, since every photon used for error correction is sent between repeater nodes in [12], their scheme would require around $20,000$ parallel channels connecting the neighboring nodes. Thus, while Ref. [12] showed the theoretical possibility of all-optical repeaters, clearly further work is needed to address their practical feasibility. These results open up a compelling line of research to investigate improved all-photonic repeater architectures of various genres which could be built with practically feasible resources, and also a thorough comparative study of rates achievable with each such all-optical repeater scheme.

B. Main results

Our contributions in this paper are twofold. The first is a rigorous analysis of: (a) the secret key rates achievable with the the aforesaid all-photonic repeater architecture given the size of the clusters generated at each repeater station, and (b) the resources required (e.g., number of single photon sources and detectors required at each repeater node) to build that cluster, while taking into account in explicit detail each step in building the required clusters using a network of passive linear optics (i.e., beamsplitters and phase shifters), imperfect on-demand sources with loss (see section II for a description of the source), single photon detectors (with some number resolving capability), and feed-forward. We find that the achievable secret key rate scales as $D\eta^s$ bits/mode, where D and $s < 1$ are functions of the number of photon sources at each repeater node (the resource constraint—which is parametrically related to the size of the cluster), all the 'inline' losses (e.g., losses in the optical fiber or waveguide used while creating the cluster, independent of the fiber loss between repeater stations), and the source and detector efficiencies. With $\eta \sim e^{-\alpha L}$ in fiber, the key rate still scales exponentially with L, but with a smaller exponent compared to the best direct-transmission protocol. This is no surprise given the analysis of [11], since the tree-cluster construction of [12] essentially mimics an imperfect quantum memory, but one whose efficiency cannot simply be modeled by a constant per mode as in Ref. [11]. Using the cluster building scheme proposed by Li et al. [16], we find that to a good approximation, the resource requirements are determined by the number of probabilistic fusion steps k required to build the cluster starting from single photons, and hence, we calculate the performance with the best cluster that can be built in k fusion steps. We use the scheme of Li *et al.* because it has been shown to be more efficient than the scheme of Varnava *et al.* [15] at building clusters [16]. Given all the inline and device losses, we evaluate the number of photon sources (and detectors) needed at each repeater node to beat $R_{\text{direct}}(L)$ at a given total range L between Alice and Bob. We also prove that given the device losses, there is an optimal spacing between the repeater nodes (which evaluates to roughly 1.5 km for a set of system parameters we choose), regardless of the overall range L.

Our second major contribution in this paper is a significant improvement to the all-photonic repeater architecture in [12]—both in terms of the resources required at each node and the number of parallel optical channels connecting the neighboring nodes. We find that barely beating $R_{\text{direct}}(L)$ using the all-optical scheme of [12] requires more than 10^{11} photon sources at each repeater node for realizing the required optical cluster states and measurements. It also requires 208 parallel channels connecting neighboring nodes, even when assuming very optimistic device-loss parameters. Assuming the same device losses, our improved repeater architecture reduces the number of photon sources (to barely beat $R_{\text{direct}}(L)$) by 5 orders of magnitude, while reducing the number of parallel channels to 8. In both of these calculations, each source is used only once per clock cycle, i.e., they are not temporally multiplexed. We prove a tight analytical lower bound for the performance of our improved scheme. These performance advances are enabled primarily by the following: (1) using boosted fusion logic that improves the success probability of the BSM to 75% by using four ancilla single photons [17], (2) employing a more resource-efficient scheme for creating tree clusters, building on the work of [15, 16], (3) retaining all the ancilla photons used for loss protection (i.e., to mimic a quantum memory) locally at the repeater nodes in a lossy waveguide, and (4) optimizing the timing of several single qubit measurements in the entire protocol.

We will limit our analysis to include photon losses (during the entire 'lifetime' of each photon, i.e., from the time of generation to detection) but will not consider 'multi-photon' errors stemming, for instance, from multi-photon emissions from the source, or detector dark clicks. We should note however that the error correction scheme analyzed here also provides some protection against depolarizing noise [12], a variant of which arises when one assumes multi-photon errors, and errors stemming from imperfect mode matching within the passive linear optical circuits at the repeater nodes.

The remainder of the paper is organized as follows. Section II reviews preliminaries and notation used in the paper. Section III describes our (improved) all-photonic quantum repeater architecture with a detailed description of each step starting from the creation of the tree clusters for error-protection, photon transmission, measurements at the repeater nodes, and the measurements by Alice and Bob, followed finally by key generation. Section IV derives a closed form expression for a lower bound to the rate-distance envelope (i.e., an achievable rate by the protocol), which we show (numerically) to match the true rate-distance envelope extremely closely. Section V compares our scheme to that of Ref. [12] in terms of resource requirements and rates, and discusses possible avenues for further improvement. The concluding section VI provides concrete directions for future research in order to further improve the prospects of a quantum communications network based solely on flying qubits.

II. PRELIMINARIES

In this paper, we work with dual-rail photonic qubits, where the logical $|0\rangle$ and $|1\rangle$ are encoded by a single photon in one of two orthogonal (spatial) modes. A photonic *cluster* state (or, graph state), on a graph $G(V, E)$ with vertices in set V and edges in set E, can be constructed by preparing each of the $|V|$ qubits (one stationed at each vertex) in the state $(|0\rangle + |1\rangle)/\sqrt{2}$, and applying $|E|$ controlled-phase operations (a two-qubit unitary gate that applies a pauli Z gate to the second qubit if the first qubit is in the $|1\rangle$ state and applies an identity otherwise) on each pair of vertices that share an edge [18]. The (entangled) quantum state of the $|V|$ qubits thus obtained is an eigenstate of the $|V|$ stabilizer operators $X_i \ \Pi_{j\in\mathcal{N}(i)}Z_j$, where the index i runs over all the vertices, X_i and Z_j are Pauli X and Z operators on qubit i and qubit j respectively, and $\mathcal{N}(i)$ is the set of all nearest neighbor vertices of vertex i. One simple observation, given that the cluster state is an eigenstate of the aforesaid stabilizer operators, is that an X measurement on qubit i, and Z measurements on all but one of the qubits in $\mathcal{N}(i)$, would deterministically reveal what the outcome of a Z measurement on that unmeasured qubit in $\mathcal{N}(i)$ would have been, *even if* that unmeasured qubit had been lost. This realization is at the heart of the tree-based counterfactual error correction for protection against photon losses, developed by Varnava et al. [14]. The idea is to attach a tree cluster to each physical photonic qubit in the graph state that needs to be protected against qubit loss. One can then deduce the result of any measurement on that qubit via an appropriate sequence of measurements on the qubits of the attached tree. The physical qubit and the qubits of the tree together form a protected (logical) qubit. We consider regular trees described by the *branching vector* $\vec{b} \equiv \{b_0, b_1, \ldots, b_m\}$, which signifies that the root of the tree has b_0 children nodes, and each of those nodes have b_1 children nodes, and so on until $b_0 b_1 \ldots b_m$ nodes at depth m. For such regular trees used for loss-error protection, one can write an explicit, yet recursive, expression for the success probability P of performing an arbitrary single-qubit measurement on the protected qubit [14]. It was shown that one can push P arbitrarily close to 1 as long as the probability of losing each photon is less than 1/2. Fig. 1 illustrates how to attach a $\{3, 2, 2\}$ tree, shown by the dark (purple) shaded nodes, to a physical qubit of a cluster, shown by light (green) shaded nodes. Note that after the tree cluster is attached to the physical qubit, X basis measurements must be performed on the physical qubit itself and the root node of the tree. These X basis measurements, if successful, create additional edges (shown in dashed blue in Fig. 1) between each neighboring qubit of the root node and each neighboring qubit of the physical qubit, after which the tree-protected logical qubit is ready to use.

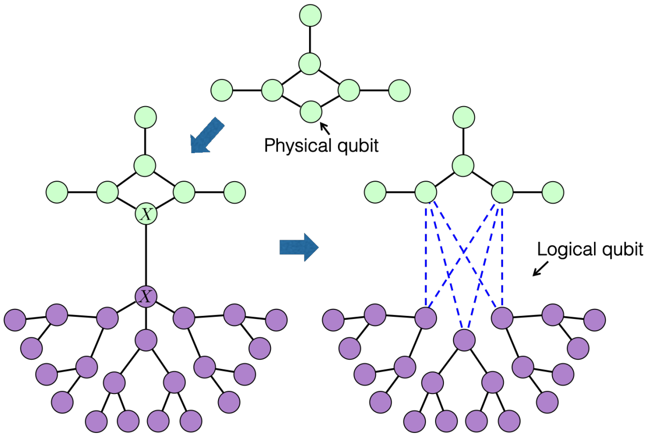


FIG. 1. Attaching a $\{3, 2, 2\}$ tree to a node of a photonic cluster.

An ideal loss-less photonic cluster state on graph G is a pure state, $|\psi\rangle_G$. A lossy cluster state on G is obtained when all the photonic qubits of $|\psi\rangle_G$ are transmitted through independent pure-loss beamsplitters each of transmissivity η. We call $1 - \eta$ the *loss rate* of such a lossy cluster state. Clearly, the loss rate of $|\psi\rangle_G$ itself is 0.

Arbitrary photonic cluster states can be prepared—with non-unity probability—using ideal single photons, passive linear optics (i.e., beamsplitters and phase shifters) and single photon detectors [19]. As examples, in the absence of losses, a two-photon maximally entangled (Bell) state can be prepared with success probability 3/16 [20], whereas a three-photon maximally entangled (GHZ) state can be prepared with success probability

1/32 [15]. Browne and Rudolph introduced linear-optical Type I and Type II two-qubit fusion gates, which if successful (with probability 1/2), can fuse two cluster fragments into one, according to specific rules [19]. These fusion gates, in conjunction with Bell states and GHZ states, can be used to construct arbitrary cluster states. The success probability of the fusion gates can be improved to 3/4 if additional (ancilla) single photons are available to be injected on-demand into an otherwise-passive linear optical circuit, and if the detectors have up to two-photon number resolution [17]. We assume such *boosted* fusion gates in our all-optical repeater construction described in this paper.

We model a lossy single photon source of efficiency η_s as one that emits, on demand, the mixed state $\eta_s \left|1\right\rangle \left\langle 1\right| + (1-\eta_s) \left|0\right\rangle \left\langle 0\right|$. We use η_d for the efficiency of all detectors in the system. We will assume that the cluster is created on a photonic chip to allow for easier scalability after which the photons are coupled, with efficiency η_c, into fiber with loss coefficient α and speed of light c_f. $P_{\text{chip}} = e^{-\beta\tau_s c_{\text{ch}}}$ denotes the survival probability of a photon on-chip during one feed-forward step, where β is the loss coefficient, c_{ch} is the speed of light and τ_s is the feed-forward time, all on-chip. $\eta_{\text{GHZ}} = \eta_s\eta_d/(2-\eta_s\eta_d)$ is the survival rate of the photons that are input into a linear-optical circuit intended to produce 3-photon maximally-entangled GHZ states [15]. The final measurement step requires feed-forward in fiber. The survival probability, P_{fib}, during feed-forward time in fiber, τ_f, is $P_{\text{fib}} = e^{-\alpha\tau_f c_{\text{f}}}$. The values for device performance assumed for the plots that appear later in the paper, are summarized in Table I.

III. REPEATER ARCHITECTURE

Before we discuss the all-photonic repeater architecture, it is instructive to review a generic quantum repeater architecture based on multimode quantum memories, probabilistic BSMs, and multiplexing over m parallel channels depicted in Figs. 2(a) and (b), which was proposed by [10], and analyzed in [11]. The parallel channels can be a combination of mutually-orthogonal spectral, spatial, and polarization modes, over each of which dual-rail photonic qubits can be transmitted simultaneously at the clock rate (determined by the source and detector bandwidth). Alice and Bob are separated by optical fiber of length L (i.e., end-to-end transmissivity, $\eta = e^{-\alpha L}$), interspersed with n repeater stations spaced $L_0 = L/n$ apart, with Alice and Bob $L_0/2$ away from the terminal repeaters in the chain.

Each of the n repeater nodes (or, 'major nodes'), shown by a gray box, consists of a multimode quantum memory straddled between sources of m Bell pairs on its left and another m on its right. Each major node loads one half of an entangled Bell state onto the memory, while transmitting the other half towards the middle of the adjoining *elementary link*. Each major node does the above synchronously on every clock cycle. At the center of each elementary link is a 'minor node', shown as dark-blue-shaded boxes in Fig. 2(b). After the qubits from the major nodes reach the minor nodes (i.e., after propagation through a distance $L_0/2$), each minor node, simultaneously, performs BSMs on each of the m pairs of qubits received from the repeater nodes on its either side. The successful BSMs within each elementary link are shown by thick (green) line segments. Immediately after the minor node BSMs, each minor node sends back the information—about which of the m channels were successfully measured—to its two neighboring major nodes, on an authenticated classical channel. Upon receipt of that information, each major node performs a BSM on two qubits held in its memory that had been entangled halves of qubits that participated in successful BSMs at the minor node to the left of that major node, and the minor node to its right, respectively. Simultaneous with the minor-node BSMs, Alice and Bob measure, in one of the two randomly-chosen mutually-unbiased bases, the m qubits they receive at their respective ends of the terminal half-elementary-link segments (see Fig. 2(b)), and send the information about which channels generated a 'click' on their detectors, back to their respective neighboring major nodes. Finally, each major node sends the information on whether its BSM succeeded, to Alice and Bob. Hence, at every clock cycle, with some probability (i.e., if all the minor nodes heralded at least one success each, all major node BSMs were successful, and Alice and Bob both detected a photon on at least one of the m channels each while using the same measurement bases), Alice and Bob obtain a shared (raw, sifted) bit. A long sequence of sifted bits is thereafter used to distill a quantum-secure shared secret via error correction and privacy amplification.

The all-optical repeater architecture we now discuss builds upon a recent proposal by Azuma *et al.* [12], although there are some important differences, which we will point out later in Section V. The key idea is to mimic a quantum memory (whose goal is essentially to protect photonic qubits against loss for a certain time duration) by using the tree cluster approach described in Section II. The authors of [12] went one step further and subsumed the functionalities of all the subcomponents of the major node (the quantum memory as well as the $2m$ Bell pair sources) into one single giant optical cluster state, which we describe next. Fig. 2(c) illustrates the construction of this cluster. We start with a depth-2 star cluster with a degree-$2m$ root node, and $4m+1$ total qubits. The 'outer' qubits, shown as white circles, play a role analogous to the white qubits in Fig. 2(a) that are transmitted to the minor nodes on fiber channels. The $2m$ 'inner' qubits, shown as gray circles, are each attached with a tree cluster of an appropriately-chosen branching vector $\vec{b}$, thereby creating a giant tree cluster. The loss-protected (logical) inner qubits play a dual role, that of the black qubits in Fig. 2(a) that are held in the quantum memories locally at the major nodes, and that of

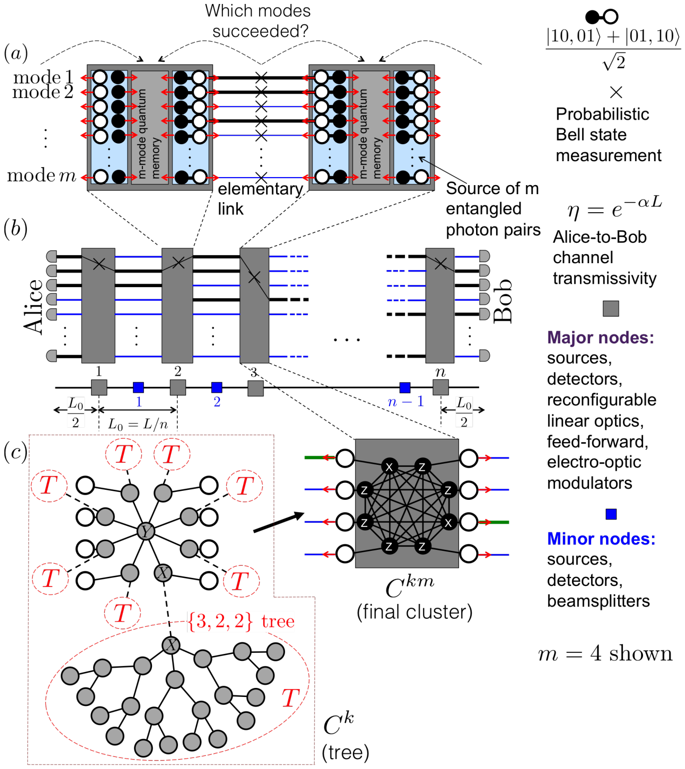

Which modes succeeded?
(a)
mode 1
mode 2
mode m
m-mode quantum memory
elementary link
Source of m entangled photon pairs
(b)
Alice
Bob
1
2
3
n
1
2
$n-1$
$\frac{L_0}{2}$
$L_0 = L/n$
$\frac{L_0}{2}$
(c)
T
Y
X
Z
$\{3, 2, 2\}$ tree
C^k
(tree)
C^{km}
(final cluster)
$\frac{|10,01\rangle + |01,10\rangle}{\sqrt{2}}$
Probabilistic Bell state measurement
$\eta = e^{-\alpha L}$
Alice-to-Bob channel transmissivity
Major nodes:
sources, detectors, reconfigurable linear optics, feed-forward, electro-optic modulators
Minor nodes:
sources, detectors, beamsplitters
$m = 4$ shown

FIG. 2. (a) and (b) show schematics of one elementary link, and a chain of them connecting Alice and Bob, respectively, for a repeater architecture that employs quantum memories, Bell pair sources, probabilistic BSMs, and multiplexing over m orthogonal parallel channels. (c) depicts the construction of a photonic cluster state that can subsume the roles of the quantum memory and the Bell pair sources, thereby resulting in a quantum repeater architecture based solely on ‘flying’ qubits. The outer (white) photonic qubits are transmitted on the fiber channels, and the inner (black) qubits are held locally in a (lossy) waveguide at the repeater node. See text for a detailed description.

the memories themselves. We make the two X measurements corresponding to each tree appended to the star, as described in the previous section (i.e., a total of $4m$ X measurements). Finally, we make a Y measurement on the root node of the star, which has an effect of creating a clique among all the (logical) inner qubits, shown by black circles in Fig. 2(c). The clique of the $2m$ logical inner qubits, connected to the $2m$ outer qubits, forms the full photonic cluster state that each major node creates every clock cycle, and sends out the $2m$ outer qubits (the white circles) towards the neighboring minor nodes (m to the left and m to the right) on fiber channels. Note that the final cluster state (after the X and Y measurements) is not a tree.

Each major node is equipped with single photon sources, reconfigurable passive linear optics, and single photon detectors. The clusters are created using linear optics and feed-forward [15, 16]. Since the cluster creation process is probabilistic, the resources (number of photon sources, detectors, size of linear optic circuit) must be chosen to ensure a near-unity success probability of creating the cluster in every clock cycle (see Fig. 5).

The minor nodes are identical to what was described earlier. The remainder of the protocol proceeds exactly as described at the beginning of this Section in the context of the memory-based architecture, except for the following difference of the action at the major nodes. When the information about which modes were successful comes back at a major node (from the two neighboring minor nodes), instead of doing a BSM between a pair of qubits held in a memory, the major node applies X measurements on the two logical inner qubits corresponding to the successful modes on either side of the clique, and makes Z measurements on the remaining $2m-2$ logical inner qubits (see Fig. 2(c)). The X measurements have the effect of fusing the successful outer qubits into an entangled chain, and the Z measurements have the effect of removing the extraneous qubits from the cluster.

So, in any given clock cycle, if the photonic clusters at each major node are successfully created (which includes success in performing the $4m$ X measurements and one Y measurement), if all the minor nodes herald at least one BSM success, if the logical (inner) qubits survive the local storage at the major nodes while the outer qubits fly to the minor nodes and the classical information (about which modes were successful) arrives back, if the two X measurements and $2m-2$ Z measurements done to prune the clusters at the major nodes using that classical information are successful, and if Alice and Bob get at least one click each while using same measurement bases, then Alicte and Bob obtain a raw sifted shared bit. In Section IV, we explicitly calculate this overall success probability, and the resulting secret-key generation rate. As we will see, larger error-protection trees afford better rate performance (up to a limit governed by the device loss rates), but creating larger clusters at the major nodes requires more resources (sources and detectors).

In Section III A, we describe in detail the construction of the clusters at the major nodes using linear optics, and calculate the success probability. In Section III B, we will describe how the measurements on the major-node clusters are done, after the BSMs at the minor nodes, to stitch together an end-to-end entangled state between Alice and Bob.

A. Constructing the clusters at the major nodes

The cluster as described above, prepared at each major node in every clock cycle, is pieced together by fusing single photons into progressively larger cluster fragments, probabilistically, using linear-optical circuits and photon detectors. The optimal algorithm for creating photonic cluster states using linear optics—in terms of minimizing the total number of photons consumed and maximizing the eventual probability of success—is not known even for a general N-node line cluster. With losses from sources detectors and waveguides during cluster construction, finding the optimal recipe becomes even harder. One design knob is the number of redundant cluster fragments attempted at each step. A higher number of attempts improves the probability of successfully creating the final cluster, but with a higher number of required photon sources and detectors. We refer to this trick of attempting the creation of multiple identical cluster fragments at each step of the process as *multiplexing*.

We now describe the resource counts and success-probability calculations for two methods to create the cluster at the major node. The first one is a method implied by previous rough estimates of the resource requirements [15, 16]. We then discuss an improved scheme that decreases the resource requirements during the creation process. Fig. 4 provides a schematic for these two schemes, which we refer to in the discussion below.

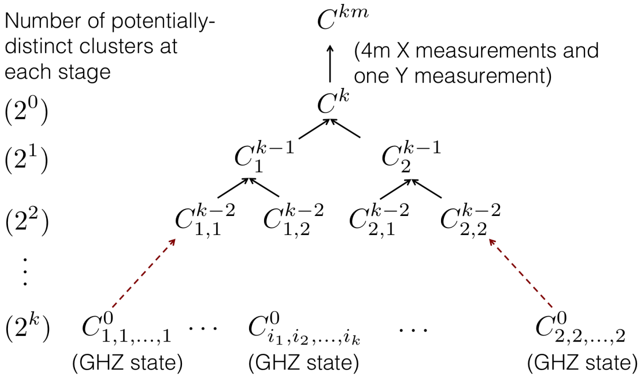


FIG. 3. The tree cluster C^k (and the final cluster C^{km} after the X and Y measurements), shown in Fig. 2, are created by a sequence of probabilistic linear-optical fusion-II operations, starting from 3-photon maximally-entangled (GHZ) states.

Let us label the final cluster C^{km} (see Fig. 2) where the letter m signifies that the Y measurement required to turn the inner qubits of the star into a clique (a fully interconnected graph) and the X measurements required to connect the error protection trees to the inner qubits have already been applied. Before these measurements, the (tree) cluster is labelled as C^k. We label the daughter clusters that are fused together to create C^k as C_1^{k-1} and C_2^{k-1}. The daughter clusters that are fused together to create C_1^{k-1} are: $C_{1,1}^{k-2}$ and $C_{1,2}^{k-2}$. The clusters that are fused together to create $C_{1,2}^{k-2}$ are: $C_{1,2,1}^{k-3}$ and $C_{1,2,2}^{k-3}$, and so on (See Fig. 3). At the bottom of the stack are 3-photon GHZ states, $C_{\boldsymbol{i}}^0$ with $\boldsymbol{i} \equiv i_1, i_2 \ldots, i_k$, which are in turn created by groups of 6 photons fed into linear-optical circuits that generate the 3-photon GHZ states with probability $P_{\rm GHZ} = \left[\eta_s\eta_d(2-\eta_s\eta_d)\right]^3/32$ [15]. The loss rate of the heralded GHZ states is, $1-\eta_{\rm GHZ}$ where $\eta_{\rm GHZ} = \eta_s\eta_d/(2-\eta_s\eta_d)$ [15].

We assume that the cluster C^k can be prepared in a series of k fusion steps, where at each step, clusters of roughly equal sizes are fused together, thus roughly doubling the cluster size in each step [16]. This assumption becomes accurate in the limit of large clusters. This method ties the final size of the intended cluster ($N_{\rm cluster} = 2^k + 2$ photons) to the number of fusion steps (k), and this relationship becomes increasingly exact as k becomes large. In other words, we assume that $C_{\boldsymbol{i},1}^{l-1}$ and $C_{\boldsymbol{i},2}^{l-1}$ are two clusters each of p photons, which when fused successfully using a fusion-II gate (applied to one photon each of the above two clusters) creates the $2p-2$ photon cluster $C_{\boldsymbol{i}}^l$, $\boldsymbol{i} \equiv i_1, i_2 \ldots, i_{k-l}$. Starting with the 3-photon GHZ states $C^0_{i_1,i_2\ldots,i_k}$, the size of C^k is 2^k+2 photons. Hence, the minimum number of fusion steps required to build a $N_{\rm cluster}$ photon cluster is $k = \lceil \log_2(N_{\rm cluster}-2)\rceil$. The label k, the number of fusion-II steps used to arrive at C^k, also translates to the resource requirements, and the loss rate of each photon in the final cluster, as we show below. Note that k is a function of the branching vector $\vec{b}$ of the error-correction trees used. The larger the error-correction trees, the larger is the final cluster C^k, and the larger is the number of steps k required to prepare that cluster.

1. *The naive multiplexing scheme*

Let us now examine the cluster creation process (depicted for $k=2$ in Fig. 4(a)). At every point we need the cluster fragment $C_{\boldsymbol{i}}^l$, we attempt to create n_B copies of that identical cluster ($n_B = 3$ shown in Fig. 4(a)), of which hopefully one is successfully created and heralded for further use. Therefore, creating one usable copy of C^k requires $(2n_B)^k$ GHZ states $C^0_{i_1,i_2\ldots,i_k}$ at the bottom of the stack. Each GHZ state is picked from $n_{\rm GHZ}$ parallel-attempted GHZ states ($n_{\rm GHZ} = 4$ shown in Fig. 4(a)), and creating each GHZ state requires 6 single photons. Therefore, creating one usable copy of C^k requires $(2n_B)^k \times 6n_{\rm GHZ}$ single photons. Finally, at the top of the chain, we create $n_{\rm meas}$ copies of C^k in parallel ($n_{\rm meas} = 4$ shown), on each of which the $4m$ X measurements and one Y measurement are performed, to prepare copies of the final required cluster C^{km}. We choose $n_{\rm meas}$ such that we obtain with high probability one successfully-created copy of C^{km}. Therefore, the total number of single photon sources (shown by black dots at the bottom of Fig. 4(a)) that need to simultaneously fire on every clock cycle, $N_s = 6n_{\rm GHZ}\, n_{\rm meas}(2n_B)^k$.

The probability of successfully creating a GHZ state $C^0_{i_1,i_2\ldots,i_k}$ is $P_0 = 1-(1-P_{\rm GHZ})^{n_{\rm GHZ}}$. The success probability of fusion at the l-th step—i.e., that of combining $C_{\boldsymbol{i},1}^{l-1}$ and $C_{\boldsymbol{i},2}^{l-1}$ into $C_{\boldsymbol{i}}^l$—is given by $Q_l = (\eta_{\rm GHZ}P^l_{\rm chip})^2/2$. The success probability of heralding one cluster $C_{\boldsymbol{i}}^l$ (from the n_B parallel copies attempted) is given by the recursive formula, $P_l = 1-(1-P_{l-1}^2 Q_l)^{n_B}$, with P_0 given as above. The $4m$ X measurements and one Y measurement required to convert C^k to the final cluster C^{km} succeed with probability $P' = \left(\eta_{\rm GHZ}P^{k+1}_{\rm chip}\right)^{4m+1}$. Since this step is multiplexed over $n_{\rm meas}$ parallel attempts, the success probability of heralding one copy of the final cluster at a major node is given by, $P_{c1} = 1 - (Q_k P')^{n_{\rm meas}}$. The success probability of all n repeater nodes creating the clusters C^{km} locally during any given clock period, is $P_{cn} = P_{c1}^n$. The blue (dashed) plot in Fig. 5 shows P_{cn} as a function of N_s for $n = 250$ repeater stations (major nodes), $k = 7$, and for device parameters as given in Table I.

2. The improved multiplexing scheme

The improved multiplexing scheme we now describe addresses the following deficiencies of the scheme described above.

- The protocol presented above does not make the most optimal use of the multiple copies of identical clusters that are successfully created at a given step. To illustrate this point, let us consider the $n_B = 3$ copies of (attempted) C^2 clusters that are shown in Fig. 4(a), of which one successfully created C^2 is picked. The first of those three attempted C^2 clusters is shown to be created by fusing a C_1^1 cluster and a C_2^1 cluster. The C_1^1 is chosen out of $n_B = 3$ copies of (attempted) C_1^1 clusters, as shown. If two of those three copies of C_1^1 are actually successfully created, the second success goes waste. Note however that the second and the third (of the three attempted) C^2 clusters also each need to be created by fusing a C_1^1 and a C_2^1. Those two C_1^1 clusters are also picked from $n_B = 3$ copies each of (attempted) C_1^1 clusters (not shown in the figure). It is thus simple to see that at each time step, a total of $(n_B)^k = 9$ copies of C_1^1 are attempted, but the selection of successes only happen within groups of three, which is clearly inefficient. A far more efficient approach is to maintain one single "bank" of copies of C_1^1 and similarly one single bank for copies of C_2^1, and attempt fusions on clusters from these two banks pairwise (and throw away the excess clusters in the bank that has more copies), to produce a single bank of C^2 clusters. This way, one does not have to choose the multiplexing numbers n_B, $n_{\rm GHZ}$ and $n_{\rm meas}$, and the total number of single photons N_s directly translates to an overall probability of success P_{c1} of creating the final cluster C^{km}. In general, we maintain single banks of each distinct cluster fragment consumed in the entire stack shown in Fig. 3, and for each fusion step shown in Fig. 3, we apply pairwise fusion to *all* cluster copies from the two banks corresponding to the two daughter clusters (and throw away the excess clusters from the bank that has more).
- The X and Y measurements that were performed at the very end (on $4m+1$ nodes of the tree cluster C^k, to convert it to the required final cluster C^{km}) can be performed at the very beginning—on the appropriate photons (which would eventually become those $4m+1$ photons in C^k)—while they are still part of the 3-photon GHZ states, i.e., before any of the fusion-II operations begin. Making these measurements at the bottom of the stack makes failures much less costly, which in turn significantly reduces the resource requirements (i.e., the N_s required to achieve a given final success probability $P_{\rm cn}$). Appendix A rigorously explains why these measurements can be done on the photons while they are still parts of the GHZ states.
- The success probability of each of the fusion-II operations (at all k steps in the cluster creation process) can be improved from 1/2 to 3/4 by injecting ancilla single photons [17]. These success probability numbers diminish with source and detection inefficiencies. But, the cost of using additional photons needed (as ancillas) to realize these *boosted* fusion gates is far outweighed by the effect of the success-probability improvement, thereby improving the effective tradeoff between N_s and $P_{\rm cn}$.

We start with N_s photons and send them all through GHZ factories, hence attempting the creation of $\lfloor N_s/6 \rfloor$ 3-photon GHZ states. The number of GHZ states x successfully created follows a binomial distribution $B(x, \lfloor N_s/6 \rfloor, P_{\rm GHZ})$ where $B(x,n,p) = \binom{n}{x} p^x (1-p)^{n-x}$. Hereonafter, let us follow an illustrative set of numbers for a $k = 2$ cluster, which is depicted schematically in Fig. 4(b). Suppose we get $x = 18$ successfully-created GHZ states. These GHZ states are now split into 4 banks corresponding to $C_{1,1}^0$, $C_{1,2}^0$, $C_{2,1}^0$ and $C_{2,2}^0$. Out of these, let us say $C_{1,1}^0$ and $C_{2,2}^0$ consist of photons that would be eventually measured in C^k. As discussed in Appendix A, these qubits can be measured now. Since the measurement of photons has a success probability $P_{\rm chip}\eta_{\rm GHZ}$, the number of $C_{1,1}^{0m}$ cluster states (x) created as a result of making measurements on y $C_{1,1}^0$ states follows a binomial distribution $B(x, y, P_{\rm chip}\eta_{\rm GHZ})$. The banks corresponding to $C_{1,1}^0$ and $C_{2,2}^0$ are given a fraction $1/(P_{\rm chip}\eta_{\rm GHZ})$ more GHZ states. Hence, these banks have 5 GHZ states each whereas the other two have 4 each. Suppose that measuring the 5 copies of $C_{1,1}^0$ results in 4 copies of $C_{1,1}^{0m}$, and measuring the 5 copies of $C_{2,2}^0$ results in 4 copies of $C_{2,2}^{0m}$. The first fusion step is now attempted (i.e., fusing $C_{1,1}^{0m}$ with $C_{1,2}^0$, and fusing $C_{2,1}^0$ with $C_{2,2}^{0m}$) resulting in 2 successfully created copies of C_1^{1m} and 3 copies of C_2^{1m} (the maximum possible number of successes in both cases was 4). In the final step, there are 2 fusion attempts from which we get one copy of the final cluster state C^{2m}.

In general, in a level-l fusion step in Fig. 3, and with y_1 and y_2 copies in the respective banks of the two daughter clusters, the distribution of the number x of fused states $C_{\boldsymbol{i}}^l$ is, $B\left(x, \min\{y_1, y_2\}, p_l\right)$, where $p_l = \mu_l^2 \left(\frac{1}{2}(\eta_s\eta_d)^2 + \frac{1}{4}(\eta_s\eta_d)^4\right)$ [17] and $\mu_l = \eta_{\rm GHZ} P_{\rm chip}^{l+1}$ is the survival rate of photons up to before the l^{th} fusion step. The success probabilities of this scheme, P_{c1} (and P_{cn}) are calculated using Monte Carlo simulations.

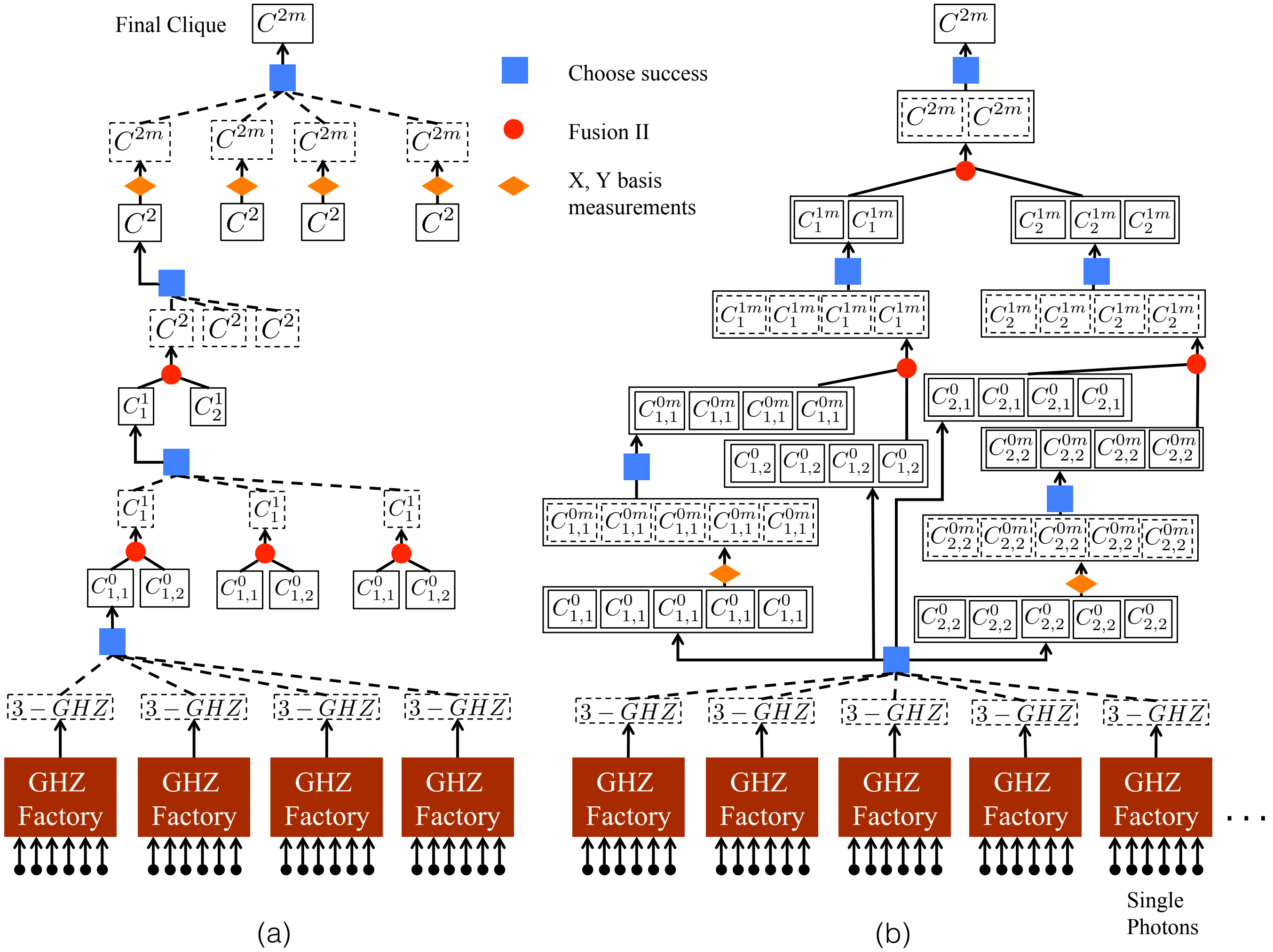


FIG. 4. (a) the naive multiplexing scheme. A dashed rectangle represents a cluster that has some probability of having been been created after a probabilistic fusion step (red circle) or at the output of creating GHZ states using linear optics starting from six single photons (labeled 'GHZ Factory'). A solid rectangle represents a cluster state that is successfully created with high probability by choosing a successful outcome (blue square) out of several identical copies attempted (dashed boxes). (b) the improved multiplexing scheme. A box surrounding clusters of the same type represents a bank of clusters and any operation applied to the bank is applied to all the clusters in it.

In Fig. 5, we plot the probability P_{cn} of successfully building clusters C^k (with $k = 7$), simultaneously at $n = 250$ major nodes, for both schemes. n_B, $n_{\rm GHZ}$ and $n_{\rm meas}$ are optimized for the naive scheme to maximize P_{cn} for any given N_s. The plot clearly shows that the improved scheme leads to resource savings by a factor of $\sim 10^4$. We further observe that, for both schemes, P_{cn} undergoes a rapid percolation-like transition from zero to one as N_s is increased beyond a certain threshold value. P_{cn} is only a function of k, n, and N_s. We fix $P_{cn} = 0.9$ and calculate the corresponding minimum N_s required, for every value of k and n. This sharp-transition behavior of P_{cn} allows us to conveniently split the problem of designing the repeater architecture into two parts:

(1) choosing an error-protection level by choosing m (number of parallel qubit channels) and $\vec{b}$ (the branching vector of the error protection trees), which gives us k (indicative of the total cluster size), and using this to calculate the key rate vs. distance achieved—both with n repeater stations, and also the resulting envelope over all n; and

(2) given the design choices (m and $\vec{b}$), calculating the number of photon sources N_s so as to achieve a close-to-unity P_{cn} (probability that all n nodes create the required clusters on every clock cycle), for a given value of k (cluster size at each repeater node), and n (the number of repeater nodes).

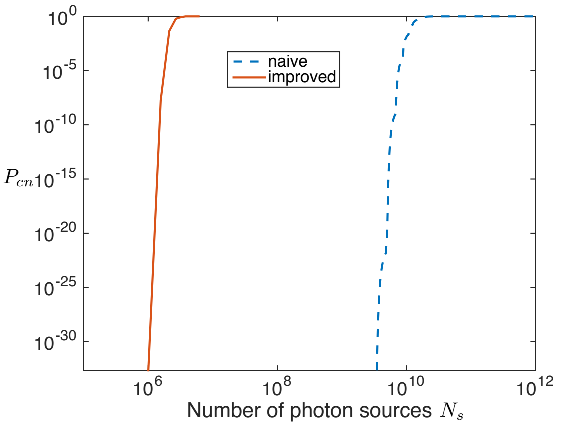


FIG. 5. The probability that all $n = 250$ major nodes are simultaneously successful in creating clusters of size $k = 7$ fusion steps (i.e., $2^k + 2 = 130$ photon clusters), using the naive and the improved multiplexing schemes.

B. Measuring the clusters and connecting the chain

Once the clusters are created, the outer qubits are sent to minor nodes at the middle of the elementary links, as shown by the arrows in Fig. 2(c). The outer qubits are measured in the Bell basis at the minor nodes using ancilla-assisted boosted fusion gates [17]. The loss rate seen by the outer qubits is $\epsilon_{\rm trav} \equiv 1 - \eta^{\frac{1}{2n}} P_{\rm chip}^{k+2} \eta_{\rm GHZ}\eta_c$ where $\eta^{1/2n}$ is the transmissivity of half of an elementary link (of range $L/2n$). All the physical qubits corresponding to the inner (logical) qubits are stored locally in a fiber bundle with the same attenuation as the communication fiber between the repeater stations. Due to the classical-communication delay, the core qubits see more loss than the outer qubits do, which we define as $\epsilon_{\rm stat} = 1 - \eta^{\frac{1}{n}} P_{\rm chip}^{k+2} P_{\rm fib}\eta_{\rm GHZ}\eta_c$. However, it is important to note that, just like in the architecture of [10, 11], this delay only leads to a latency in the scheme and does not affect the clock rate of the system.

When the result of the BSMs on the m qubit channels at the two neighboring minor nodes arrive back at a major node, the major node picks one successful qubit channel on either side (if none of the m BSMs were a success on any one of the sides, then that time period is an overall failure). The logical inner qubits corresponding to all the outer qubits that are not deemed part of the successful BSMs are removed from the cluster by measuring them in the Z basis [14] (note that this Z measurement is a logical one, which benefits from the loss-protection trees). On the two logical qubits (one on either side) corresponding to the successful channels, X basis measurements are performed, which has an effect of extending the entanglement. Alice and Bob, simultaneous with the minor node BSMs, detect the m outer photons sent to them by the first and the last major node in the repeater chain, over links of length $L_0/2$, using one of two randomly-chosen mutually-unbiased bases. Assuming the clusters at all n repeater nodes were successfully created (which happens with probability P_{cn}), the conditional probability of generating an end-to-end entangled pair between Alice and Bob, in one clock cycle, is given by the probability that all $n-1$ minor nodes herald at least one successful BSM, and all the pruning logical X and Z measurements on the clusters at all n major nodes are successful, and Alice and Bob both obtain successful detects on at least one of the m qubit channels:

$$P_{\rm meas} = P_Z^{2(m-1)n} P_X^{2n} \left[1 - (1 - P_B)^m\right]^{n-1} P_{\rm end}^2, \quad (1)$$

where P_X and P_Z are the probabilities of successful X and Z basis measurements on the logical inner qubits, respectively. $P_{\rm end}$ is the probability that Alice (resp., Bob) obtains at least one successful detection in one of the m qubit channels.

We quantify the performance of the repeater architecture in terms of the number of shared secret bits generated per mode (i.e., per clock cycle per spatial channel, where m is the number of spatial channels employed). Since, the channel noise comprises of only photon loss, the success probability divided by the number of spatial channels per attempt is the secret key rate (in bits per mode) generated by this scheme, i.e., $R = P_{cn}P_{\rm meas}/2m$ bits/mode. Note that the bits per mode is obtained by dividing by the number of spatial channels that is twice the number of qubit channels ($2m$). This is because we assume single-polarization dual-rail encoding where each qubit on any given spatial channel occupies two successive temporal modes.

IV. RATE CALCULATIONS

In this Section, we evaluate the secret key rate achievable using the all-optical repeater architecture described above, while accounting for all the device and channel losses. We first evaluate an expression for $R_n^{(m,\vec{b})}(L)$, the bits-per-mode rate for a given choice of design parameters: m (the number of parallel channels) and $\vec{b}$ (branching vector of the error-protection trees). L is the Alice-to-Bob range and n is the number of equally-spaced repeater nodes that are deployed between Alice and Bob. We evaluate the rate-vs.-distance envelope $R^{(m,\vec{b})}(L)$—the maximum of $R_n^{(m,\vec{b})}(L)$ at any L over the choice of $n \in \{1, 2, \ldots\}$—and we show explicitly for when $\vec{b}$ is a depth-2 tree, that $R^{(m,\vec{b})}(L) \geq D\eta^s$, with D a constant, $\eta = e^{-\alpha L}$ and s strictly less than 1. We find by numerical evaluation that this lower bound is tight. We compare this rate-distance envelope with the best rate achievable without the use of quantum repeaters $R_{\rm direct}(L) = -\log_2(1-\eta)$, for some $(m, \vec{b})$ pairs.

A given choice of m and $\vec{b}$ determines k, the number of fusion steps required to prepare the final cluster

C^k prepared by each repeater node at every clock cycle, which in turn quantifies the size ($N_{\text{cluster}} = 2^k + 2$ photons) of C^k. Next, we choose a value of k—a single parameter that quantifies the amount of resources we are willing to dedicate to each repeater node—, and numerically optimize the choice of m and $\vec{b}$ that is consistent with the chosen k, and which maximizes the rate. We denote the rate attainable with n repeater nodes conditioned on the per-node-resource-constraint parameter k, as $R_n^{(k)}(L)$ and calculate the optimal rate-vs.-distance envelope $R^{(k)}(L)$ by taking an envelope over the choice of n. Finally, we compare the rate-distance envelopes for increasing values of k and translate the values of k to the number of single photon sources required at each repeater node.

The probabilities of fault-tolerant X and Z measurements on one of the (logical) inner qubits of a major node cluster, P_X and P_Z, can be expressed in terms of the probabilities ξ_i of a successful 'indirect' Z measurement (as described in Section II) on a qubit at the i-th level of the error-protection tree [12, 14]:

$$P_X = \xi_0, \text{ and} \tag{2}$$

$$P_Z = (1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}}\xi_1)^{b_0}, \tag{3}$$

where,

$$\xi_i = 1 - \left[1 - (1 - \epsilon_{\text{stat}})(1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}}\xi_{i+2})^{b_{i+1}}\right]^{b_i}, \tag{4}$$

and $i \leq l$, $\xi_{l+1} = 0$, $b_{l+1} = 0$.

Let us assume a tree depth of $d = 2$, i.e., $\vec{b} = [b_0\ b_1]$, which is consistent with our numerical findings on the optimal branching vector as described later in the paper (see table II). For a depth-2 branching vector, using Eq. (4), we find that $\xi_0 = 1 - \left[1 - \left(1 - \epsilon_{\text{stat}}\right)^{b_1+1}\right]^{b_0}$ and $\xi_1 = 1 - \epsilon_{\text{stat}}^{b_1}$. Thus,

$$P_X = 1 - \left[1 - \left(\eta^{\frac{1}{n}}\right)^{b_1+1} B^{b_1+1}\right]^{b_0}, \text{ and} \tag{5}$$

$$P_Z = \left[1 - \left(1 - \eta^{\frac{1}{n}} B\right)^{b_1+1}\right]^{b_0}, \tag{6}$$

and the Bell measurement success probability becomes

$$P_B = \frac{AB^2}{m}\eta^{\frac{1}{n}}, \tag{7}$$

where $A = m\left(\frac{1}{2}(\eta_s\eta_d)\right)^2 + \frac{1}{4}(\eta_s\eta_d)^4)/P_{\text{fib}}^2$, $B = P_{\text{chip}}^{k+2}P_{\text{fib}}\eta_{\text{GHZ}}\eta_c$.

The probability of at least one successful detection at Alice's (or Bob's) end is given by

$$P_{\text{end}} = 1 - \left(1 - \eta^{\frac{1}{2n}} C\right)^m, \tag{8}$$

where $C = P_{\text{chip}}^{k+2}\eta_{\text{GHZ}}\eta_c$.

We now have the bits-per-mode rate achievable with an n-repeater-node chain,

$$R_n^{(m,\vec{b})}(L) = \frac{P_{cn}}{2m} P_{\text{end}}^2 P_Z^{2(m-1)n} P_X^{2n} \left[1 - (1 - P_B)^m\right]^{n-1}, \tag{9}$$

with P_X, P_Z, P_B and P_{end} as given in Eqs. (5), (6), (7) and (8), with $\eta = e^{-\alpha L}$ the transmissivity of the end-of-end channel (of range L). See the dotted magenta curves in Fig. 6 for the plots of $R_n^{(m,\vec{b})}(L)$ as a function of L for a few chosen values of n.

One way to obtain a lower bound of the envelope over the plots $R_n^{(m,\vec{b})}(L)$ over all choices of n (see black plot in Fig. 6), is to pick one point $(L_n, R_n^{(m,\vec{b})}(L_n))$ on each of the rate-distance functions $R_n^{(m,\vec{b})}(L)$, $n = 0, 1, 2, \ldots$, and connect them. Let us choose L_n as:

$$L_n = nz\ln(AB^2)/\alpha, \tag{10}$$

with z being a constant that is yet to be chosen. The Alice-to-Bob channel transmissivity at these range values are therefore given by:

$$\eta_n = e^{-\alpha L_n} = e^{-nz\ln(AB^2)}. \tag{11}$$

We now evaluate a locus of the (range, rate) pairs $(L_n, R_n^{(m,\vec{b})}(L_n))$ over $n \in \{0, 1, 2, \ldots\}$ and choose the parameter z we left undetermined in Eq. (11) so as to maximize the rate-distance envelope. We call this rate-distance envelope $R_{\text{LB}}^{(m,\vec{b})}(L)$ since this is by construction a lower bound on the true envelope $R^{(m,\vec{b})}(L)$.

Let us evaluate P_X, P_Z, P_B and P_{end} at $\eta = \eta_n$ (i.e., substitute $\eta^{1/n} = \left(AB^2\right)^{-z}$ in the respective expressions) and define the following quantities:

$$p_X = 1 - \left[1 - \left(AB^2\right)^{-z(b_1+1)} B^{b_1+1}\right]^{b_0}, \text{ and} \tag{12}$$

$$p_Z = \left[1 - \left(1 - \left(AB^2\right)^{-z} B\right)^{b_1+1}\right]^{b_0}, \tag{13}$$

$$p_B = \frac{1}{m}\left(AB^2\right)^{1-z}, \text{ and} \tag{14}$$

$$p_{\text{end}} = 1 - \left(1 - \left(AB^2\right)^{-z/2} C\right)^m, \tag{15}$$

using which let us define the following: $q_1 = p_Z^{2(m-1)}p_X^2$, $q_2 = 1 - (1 - p_B)^m$, and $q_3 = p_{\text{end}}^2$, and obtain:

$$R_n^{(m,\vec{b})}(L_n) = (q_1q_2)^n \frac{q_3P_{cn}}{2mq_2}. \tag{16}$$

To obtain the envelope $R_{\text{LB}}^{(m,\vec{b})}(L)$, we need to calculate the locus of the distance-rate pairs $(L_n, R_n^{(m,\vec{b})}(L_n))$ over $n \in \{1, 2, \ldots\}$. We do this by eliminating n from

Eqs. (10) and (16). With a little algebra, and expressing the envelope in terms of $\eta = e^{-\alpha L}$, we get the following:

$$R_{\mathrm{LB}}^{(m,\vec{b})}(\eta) = D\eta^{s}, \tag{17}$$

where $D = \frac{q_3 P_{cn}}{2mq_2}$ and the exponent $s = -\frac{\ln(q_1 q_2)}{z\ln(AB^2)}$.

Note that $R_{\mathrm{LB}}^{(m,\vec{b})}(L)$ in (17) is a lower bound on the actual rate-distance function $R^{(m,\vec{b})}(L)$ for any value of the parameter z that we left undetermined in our choice of the range values L_n we used to evaluate $R_{\mathrm{LB}}^{(m,\vec{b})}(L)$. We numerically optimize the choice of z such that the value of the exponent s is minimized (note that q_1, q_2 and q_3 are all functions of z).

In Fig. 6, we plot $R_n^{(m,\vec{b})}(L)$ (bits per mode) as a function of L (km) for $n = 1, 10, 24, 56, 133$, and 314 (magenta dotted plots), with $\vec{b} = \{7, 3\}$ and $m = 4$, and other device parameters as summarized in Table I. These values of m and $\vec{b}$ translate to $k = 8$, i.e., $2^8 + 2 = 258$ photon clusters created at each node at every clock cycle. We also plot the analytical rate-envelope lower bound in Eq. (17), $R_{\mathrm{LB}}^{(m,\vec{b})}(L)$ (black solid line), with the optimal z computed numerically. For the chosen parameters, we get $D = 0.11$ and $s = 0.37$. The analytical lower bound $R_{\mathrm{LB}}^{(m,\vec{b})}(L)$ is visually indistinguishable at the scale of the plot from the numerically-obtained rate-distance envelope $R^{(m,\vec{b})}(L)$. This excellent agreement persists for all values of m and $\vec{b}$ we have have tried.

One interesting implication of the range values L_n in Eq. (10) lying on the rate-distance envelope is that the distance between each repeater (major) node,

$$L_0 \equiv \frac{L}{n} = \frac{\ln(AB^2)}{\alpha} \tag{18}$$

is a constant and independent of the total range L. In other words, given the device parameters and the choice of the major-node cluster size (i.e., m and $\vec{b}$), there is an optimal gap with which repeaters should be placed—no more, and no less. For the numbers used for the plots in Fig. 6, $L_0 = 1.49$ km. Fig. 6 also shows $R_{\mathrm{direct}}(L)$ for comparison (blue dashed plot), which the repeater scheme is seen to outperform beyond a range of 87 km.

As shown by the above example, our repeater scheme, even when built with lossy components, can achieve $s < 1$ i.e. it outperforms the optimum repeater-less rate $R_{\mathrm{direct}}(L)$. The value of the exponent s achievable by the repeater scheme can be improved (lowered) by enhancing the level of error correction (i.e., choosing a larger $\vec{b}$). Doing so increases the size of the clusters ($2^k + 2$ photons) needed at each repeater nodes, and hence increases the number of photon sources N_s required locally at each node. In Fig. 7, we plot the $R^{(k)}(L)$, numerically-evaluated envelopes of the rate-distance functions $R_n^{(k)}(L)$, parametrized by the single parameter k that quantifies the size of the clusters prepared by the repeaters at each clock cycle. It is seen that the rate-distance exponent s improves (decreases) as k increases.

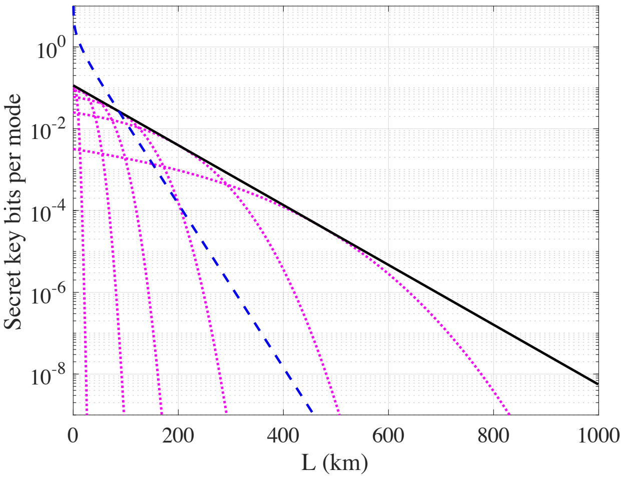


FIG. 6. The key rate (in bits per mode) $R_n^{(m,\vec{b})}(L)$ achieved by an n-node repeater chain shown as a function of range L, for $n = 1, 10, 24, 56, 133$, and 314 (magenta dotted plots), with $m = 4$ parallel channels and $\vec{b} = \{7, 3\}$ trees. The analytical lower bound to the rate-distance envelope $R_{\mathrm{LB}}^{(m,\vec{b})}(L)$ (black solid plot) is seen to surpass the best-possible repeaterless-QKD rate $R_{\mathrm{direct}}(L)$ (blue dashed plot) at $L = 87$ km.

Device parameter	symbol	value
fiber loss coefficient	α	0.046 km^{-1} (0.2 dB/km)
on-chip loss coefficient	β	0.62 m^{-1} (2.7 dB/m)
feed-forward time in fiber	τ_f	102.85 ns
feed-forward time on-chip	τ_s	20 ps
chip to fiber coupling efficiency	η_c	0.99
source detector efficiency product	$\eta_s\eta_d$	0.99
speed of light in fiber	c_f	$2 \times 10^8 m/s$
speed of light on chip	c_{ch}	$7.6 \times 10^7 m/s$

TABLE I. Assumed values for device performance parameters. The source detector efficiency product $\eta_s\eta_d$ is sufficient for the purposes of the calculations in this paper, and need not be specified separately. Recall that $P_{\mathrm{chip}} = e^{-\beta\tau_s c_{\mathrm{ch}}}$, $P_{\mathrm{fib}} = e^{-\alpha\tau_f c_f}$, and $\eta_{\mathrm{GHZ}} = \eta_s\eta_d/(2 - \eta_s\eta_d)$. τ_f has been chosen to make $P_{\mathrm{chip}} = P_{\mathrm{fib}}$.

V. DISCUSSION

In this Section, we go back to the all-photonic repeater architecture proposed by Azuma *et al.* [12], and discuss the main modifications (improvements) we considered in the architecture we described and analyzed above. We also show a comparative study of the resource requirements and rate performance of the naive scheme and our modified scheme. Following are the salient differences between the architecture we analyzed above, and the one proposed in [12].

Retaining vs. transmitting the clusters—In the proposal of [12], all the logical inner qubits, along with the outer qubits (i.e., all the N photons of the cluster at a major node) are sent to the minor node, whereas we store the inner qubit photons in a fiber spool locally at the major nodes. The former has an advantage that no classical communication needs to happen from minor nodes back to major nodes before the logical X and logical Z measurements are done to the logical inner qubits, since all those qubits are present locally at the minor nodes when the BSMs are performed there on outer-qubit pairs from neighboring major node clusters. The advantage of our (latter) scheme is that the number of parallel physical channels needed $(2m)$ is much smaller as compared to the number needed (N) for the scheme in [12]. For the numbers in Fig. 6, that is 8 as opposed to 208 parallel fiber channels connecting successive repeater nodes.

Difference in the bits-per-mode rate—Further, the bits per mode achieved by the architecture in [12] would be given by $P_{cn}P_{\text{meas}}/N$, whereas the bits per mode achieved by our modified architecture would be $P_{cn}P_{\text{meas}}/2m$. The P_{meas} of the former is higher (due to lower loss incurred by the photons of the logical inner qubits of the clusters as they do not need to wait in a lossy fiber spool while waiting for the classical information to fly back from the minor nodes). However, the other improvements described below more than compensate for the better P_{meas}, and the latter scheme achieves a far better bits-per-mode performance (see Fig. 7).

Linear optic vs. boosted linear optic fusion gates—We propose the use of the improved Bell-state measurement scheme of Ewert *et al.* [17] that inject four single photons to boost the success probability of the fusion-II gate. Our calculations show that the cost of using these additional ancilla photons is far outweighed by the effect of the improved success probability, in the performance of the repeater architecture, despite assuming lossy sources and detectors.

Improved multiplexing scheme for cluster generation—We use an improved multiplexing scheme to create the clusters at the major nodes, as described in Section III A and depicted in Fig. 4(b). Previous studies have estimated the resource requirements for cluster generation based on the average number of attempts required for each probabilistic steps [15, 16]. However, in order to generate the required cluster at every repeater station on every clock cycle with high probability, the resources required at each repeater station need to be greater than the number that would allow for cluster creation "on average". To our knowledge, this is the first study that explicitly looks at how probabilistic operations need to be multiplexed in a real system.

Pushing the measurements ahead during cluster creation—The single qubits measurements that do not depend on the outcomes of Bell measurements at the minor nodes, are performed before the fusion operations, directly on the photons of the GHZ states, very early during the cluster creation process.

Let us now see what the above modifications to the architecture does to the rate performance. The bits-per-mode rates for the naive and the improved schemes are plotted in Fig. 7(a) and (b), respectively. We assume device loss parameters as listed in Table I for both sets of plots. In each plot, we compute the rate-distance performance (envelopes taken over n, the number of repeater nodes) for four different error-protection levels (i.e., $k = 7, 8, 9$, and 10). For every point on each rate-distance envelope, m and $\vec{b}$ are optimally chosen (consistent with the given k). Each rate-distance plot exhibits the $D\eta^s = De^{-s\alpha L}$ behavior, and the exponent s diminishes as a higher k is chosen. For the naive scheme, the minimum k for which the repeater can beat $R_{\text{direct}}(L)$ (pink-dashed line) is $k = 8$ and the optimized clusters at the major nodes have 192 photons each. Hence, the scheme would require 208 parallel fiber links connecting successive nodes. In comparison, in the improved scheme, $k = 7$ is sufficient to beat $R_{\text{direct}}(L)$, and requires $2m = 8$ parallel fiber links. The optimal tree depth, for this $k = 7$ rate plot is found to be $d = 2$, which is consistent with the analytical development in Section IV.

Table II lists, at a range of $L = 300$ km, and for each of the cases $(k = 7, 8, 9, 10)$, the optimal values of m for the naive (m_{naive}) and new schemes (m_{new}), the optimal branching vector for the naive ($\vec{b}_{\text{naive}}$) and new schemes ($\vec{b}_{\text{new}}$), and the number of parallel fiber links needed in the naive scheme (N_{naive}). In the case of the new scheme, the number of parallel fiber links needed is simply $2m_{\text{new}}$.

k	m_{naive}	N_{naive}	$\vec{b}_{\text{naive}}$	m_{new}	$\vec{b}_{\text{new}}$
7	5	100	$\{3, 2\}$	4	$\{4, 2\}$
8	8	208	$\{4, 2\}$	5	$\{5, 3\}$
9	11	462	$\{5, 3\}$	6	$\{7, 4\}$
10	12	864	$\{7, 4\}$	8	$\{10, 5\}$

TABLE II. For $k = 7, 8, 9$, and 10, at $L = 300$ km range, m_{naive} and m_{new} are the optimal values of m for the naive and new schemes respectively. $\vec{b}_{\text{naive}}$ and $\vec{b}_{\text{new}}$ are the optimal values of $\vec{b}$ for the naive and new schemes respectively. N_{naive} is the corresponding number of parallel fiber links needed between successive repeater nodes in the naive scheme. For the new scheme, the number of parallel links is $2m_{\text{new}}$.

Let us now compare the resources (number of photons, N_s) required to build the major node clusters, for the respective cases that can (barely) beat $R_{\text{direct}}(L)$. The naive scheme requires 1.9×10^{11} photon sources at each major node, while the new scheme requires 3.3×10^6 sources, an improvement of 5 orders of magnitude (see Fig. 5). It is also interesting to note that if the primitive resources were 3-photon GHZ sources rather than single photon sources, 15 thousand GHZ sources would be required, a relatively smaller number.

Given the size of the earth, for terrestrial long dis-

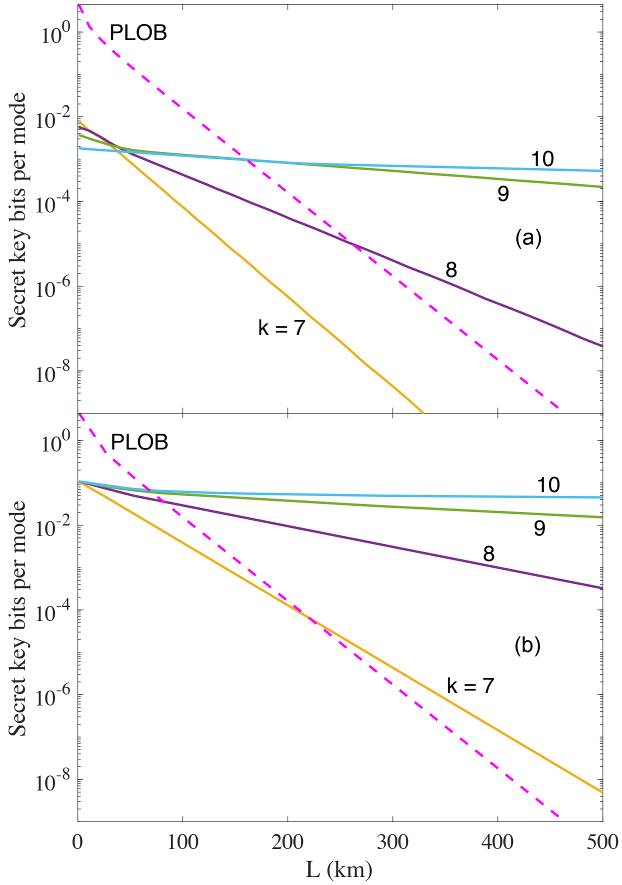


FIG. 7. The bits per mode rates $R^{(k)}(L)$ plotted for different values of k, the numbers of fusion steps, for the (a) naive scheme and (b) with the improvements of this paper. The repeater-less rate bound $R_{\text{direct}}(L)$ is the pink dashed line. $N_{\text{cluster}} = 2^k + 2$ is the total number of photons in the cluster generated at each repeater in every clock cycle.

tance communications, it is useful to quantify the performance of our (improved) all-optical repeater scheme at say 5000 km. Without quantum repeaters, the best QKD protocol realized with ideal devices cannot exceed a key rate of 2.9×10^{-99} bits per mode at this distance. Our all-optical repeater scheme, with 954-photon clusters ($k = 10$) at each repeater node can attain a key rate of 8×10^{-3} bits per mode using $2m = 18$ parallel channels and $n = 12411$ repeater nodes, which translates to a 144 kHz key generation rate assuming a 1 MHz repetition rate. If we employed 518-photon clusters ($k = 9$) instead, the rate achieved would only be 4×10^{-8} bits per mode using $2m = 14$ parallel channels and $n = 12255$ repeater nodes. The number of photon sources required at a repeater node to create the required clusters (using linear optics) for the above two example cluster-size constraints are 1.2×10^8 and 3.6×10^7, respectively.

In the presence of losses in the waveguide, there is a maximum sustainable size of the clusters at the major nodes, at least for the error protection methods described in this paper. A larger cluster requires a greater creation time and hence, each photon in the cluster sees a larger effective loss rate (stemming from the P^k_{chip} term in ϵ_{trav} and ϵ_{stat}). Since the error correction scheme has a maximum loss tolerance of 50%, there is a maximum size of the clusters that can be created and thus a maximum level of error protection that a qubit can have. So, given a set of device losses, increasing the error protection level (viz., k) cannot indefinitely improve the rate performance.

The aforesaid detrimental effect of loss with an increasing cluster size has more serious implications for cluster-state linear optical quantum computing (LOQC) in general, using the tree-based counterfactual error correction technique [14]. This is because a polynomial scaling of the number of photon sources (with the size of the cluster) is required in the asymptotic limit for the LOQC scheme to be scalable. The failure probability of every qubit needs to decrease exponentially with the size of the computation. Hence, the level of protection of each qubit must increase with the size of the problem, which implies a greater cluster creation time and hence a greater loss rate. Since there is a 50% ceiling on the tolerable photon loss with the tree code, it is not possible to achieve the required level of protection for arbitrarily large computations, as discussed above for the case of an all-photon quantum repeater. Developing a scalable method for creation of arbitrarily large clusters in constant time would solve this problem and will also allow for a polynomial scaling of the number of photons with computation size. A recent paper proposes using counterfactual error correction to fault-tolerantly create surface code data qubits [16]. However, the resource requirements for this scheme are extremely high.

VI. CONCLUSIONS

In conclusion, we have performed a rigorous analysis of the resource requirements, and the achievable secret key rates of an all-optical repeater scheme that improves upon a recent proposal [12], while taking into account all the losses in the system. While the all-optical repeater proposal of [12] presents an important conceptual advancement, we show that it may not be practically feasible given its astronomical resource requirements, both in terms of the number of photon sources and detectors needed at each repeater node, as well as the number of parallel optical fiber channels that must connect successive repeater nodes. Our scheme improves the practicality immensely in both of the aforementioned metrics, as well as the actual rate-vs.-distance performance achieved. In particular, the number of photon sources required at each node is reduced by 5 orders of magnitude, and the number of parallel channels between repeater nodes required to beat the performance of a direct-transmission QKD scheme is brought down from more than two hundred, to 8. These results suggest that further theoretical improvements on quantum photonic fault tolerant schemes may further improve the performance of all-optical quantum repeaters, as well as other applications of all-optical quantum processing. One of our major contributions in this paper was to rigorously prove that the rate-loss scaling by the aforementioned genre of all-optical quantum repeaters with a fixed cluster size is given by $R = D\eta^s$ bits per mode, where D and s are constants that are functions of various device loss parameters, and that of design choices made (to choose the level of error protection). The fact that it is possible to achieve a value as the exponent $s < 1$ proves the fact that this scheme can outperform the key rates attainable by any QKD protocol that does not employ quantum repeaters, the rate performance of which are upper bounded by $R_{\text{direct}}(\eta) \approx 1.44\,\eta$ for $\eta \ll 1$, whose linear rate-transmittance decay implies $s = 1$.

In future work, it will be interesting to incorporate more realistic effects into the resource-performance tradeoff calculations of all-optical repeaters, in particular mode-mismatch errors in the passive interferometric manipulations on the photons held locally at the repeaters, and multi-photon errors arising from imperfect sources and noisy detectors. Finally, it would be instructive to analyze and compare other forms of quantum repeater architectures, especially forward-error-corrected one-way transmission schemes [9], realized only with flying photons, linear optics and detectors, but no quantum memories.

ACKNOWLEDGMENTS

This research was funded by the DARPA project *Scalable Engineering of Quantum Optical Information Processing Architectures* (SEQUOIA), under US Army contract number W31P4Q-15-C-0045 and by the Air Force Office of Scientific Research MURI (FA9550-14-1-0052). We would like to thank Sreraman Muralidharan, Liang Jiang, Darius Bunandar, Koji Azuma, Hoi-Kwong Lo and Stefano Pirandola for helpful discussions.

Appendix A: Re-ordering measurements in the cluster-creation process

In this Section, we explain why the X measurements required to attach trees for counterfactual error correction and the Y measurement required to create the "clique" from the "star" cluster can be applied before the fusion operations. This makes the cluster creation process more efficient. The reordering of the operations is depicted in Fig. 8. Thin lines here represent photonic qubits, thick lines represent feed-forward operations, boxes labelled X, Y, Z, and H represent single qubit X, Y, Z rotations, and Hadamard gates respectively, and boxes labelled M_X, M_Y, and M_Z represent measurement in the X, Y, and Z bases, respectively.

First, we show some results regarding re-ordering of single qubit measurements and rotations. In the left side of Fig. 8(a), the unitary operation U on qubit c is conditioned on the result of an X or Y basis measurement on qubit b (that is determined beforehand). In addition, there is a conditional operation Z^i on the qubit b which depends on a feed-forward signal from a different part of the circuit, which in this case is the result of measurement M_A on qubit a. The application of a Z gate before X or Y measurement simply has the effect of flipping the result of the measurement. Hence, the measurement M_X (resp. M_Y) can be performed before M_A and the feed-forward result of M_A can simply be used to flip the result of M_X (resp. M_Y) as shown on the right side of Fig. 8(a). The system in Fig. 8(b) is identical to the system in Fig. 8(a) except for the fact that measurement in the X (resp. Y) basis is replaced by measurement in the Z basis. Since application of a Z rotation does not influence the outcome of the Z measurement, the Z gate and the associated feed-forward can be removed entirely. In Fig. 8(c), we depict that a Hadamard gate followed by an X basis measurement is equivalent to a Z basis measurement, a Hadamard gate followed by a Z basis measurement is equivalent to an X basis measurement, and a Hadamard gate followed by a Y basis measurement is equivalent to a Y basis measurement with the result flipped.

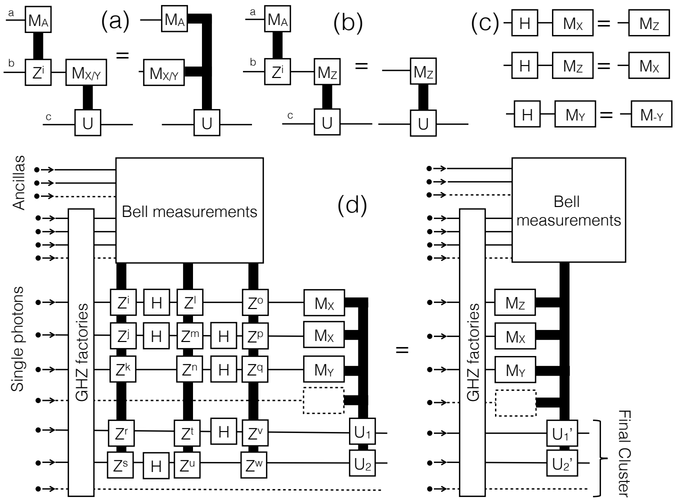


FIG. 8. Single qubit measurements can be applied before fusion operations. (a) X and Y basis measurements can be moved before conditional Z operators. (b) Z operators before Z basis measurements can be removed. (c) Hadamard gates followed by measurement in the X, Y or Z basis is equivalent to direct measurement in a different pauli basis. (d) Single qubit measurements on the final cluster can be moved before fusion operations.

We now use these results to show how measurements can be pushed earlier in the cluster creation process at the major nodes. The left side of Fig. 8(d) shows the system with measurements applied after the fusion operations. Single photons that are sent through GHZ factories to create 3-photon GHZ states, which are then fused using Bell measurements using ancilla photons. The surviving photons require some Hadamard and conditional Z rotations as part of the controlled-phase and parity-projection operations [16]. Finally, some of the surviving photons require X and Y basis measurements, the results of which are fed forward to photons in the final "clique" cluster. As shown in Fig. 8(a), (b) and (c), measurements in the Pauli basis can be pushed in front of Hadamard and conditional Z rotations by simply moving to a different Pauli basis or flipping the result of the measurement result. Hence, the system is equivalent to the right side of Fig. 8(d) in which single qubit Pauli measurements are applied before the fusion operation.

[1] M. Takeoka, S. Guha, and M. M. Wilde, Nature communications **5**, 5235 (2014).

[2] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, (2015), arXiv:1510.08863.

[3] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Physical review letters **102**, 050503 (2009).

[4] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, Physical Review Letters **81**, 5932 (1998).

[5] S. Pirandola, (2016), arXiv:1601.00966.

[6] K. Azuma, A. Mizutani, and H.-K. Lo, (2016), arXiv:1601.02933.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Physical Review Letters **70**, 1895 (1993).

[8] C. Bennett and S. Wiesner, Physical review letters **69**, 2881 (1992).

[9] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, (2015), arXiv:1509.08435.

[10] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel, Physical review letters **113**, 053603 (2014).

[11] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, Physical Review A **92**, 022357 (2015).

[12] K. Azuma, K. Tamaki, and H.-K. Lo, Nature communications **6**, 6787 (2015).

[13] M. Varnava, D. E. Browne, and T. Rudolph, New Journal of Physics **9**, 203 (2007).

[14] M. Varnava, D. Browne, and T. Rudolph, Physical Review Letters **97**, 120501 (2006).

[15] M. Varnava, D. E. Browne, and T. Rudolph, Physical Review Letters **100**, 060502 (2008).

[16] Y. Li, P. C. Humphreys, G. J. Mendoza, and S. C. Benjamin, Physical Review X **5**, 041007 (2015).

[17] F. Ewert and P. van Loock, Physical Review Letters **113**, 140403 (2014).

[18] R. Raussendorf and H. J. Briegel, Physical Review Letters **86**, 5188 (2001).

[19] D. E. Browne and T. Rudolph, Physical Review Letters **95**, 010501 (2005).

[20] Q. Zhang, X.-H. Bao, C.-Y. Lu, X.-Q. Zhou, T. Yang, T. Rudolph, and J.-W. Pan, Physical Review A **77**, 062316 (2008).

Fundamental limits and improved percolation thresholds for linear optical quantum computing using feedback-free probabilistic fusion of photonic micro clusters

Mihir Pant,[1, 2, *] Don Towsley,[3] Dirk Englumd,[1] and Saikat Guha[2]

[1] *Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139, USA*
[2] *Quantum Information Processing group, Raytheon BBN Technologies,*
10 Moulton Street, Cambridge, MA 02138, USA
[3] *Department of Computer Science, University of Massachusetts, Amherst, MA 01003, USA*

Entangled k-qubit micro clusters can be stitched together using probabilistic m-qubit linear-optic fusion operations that succeed with probability λ—without any measurement-induced feedforward—into a giant connected component (GCC) of a random percolated instance of a target lattice G, if $\lambda > \lambda_c^{(k,m)}$. The threshold $\lambda_c^{(k,m)}$ depends upon the choice of G and the sequence of fusion steps. This GCC can then be renormalized into a square-grid cluster universal for measurement based quantum computing. With two-qubit fusion operations ($m = 2$), we give an explicit construction that shows $\lambda_c^{(3,2)} \leq 0.54$. This improves over a recently published threshold of 0.625 when 3-qubit (GHZ) states are used as the initial resource; a smaller threshold on λ implies a higher resilience to device losses. We also show that $\lambda_c^{(k,2)} \geq 1/(k-1)$ for all $k \geq 2$. With 3-qubit (GHZ) states as the initial resource, $\lambda_c^{(3,2)} \geq 0.5$, which implies that a fusion gate based on passive linear optics will not work (due to its 0.5 success-probability limit) and that one must use fusion gates boosted with injected single photons or 2-qubit entangled Bell states. Further, with 2-qubit (Bell) states as the initial resource, ballistic linear-optical quantum computing is practically impossible using pairwise fusion operations, since $\lambda_c^{(2,2)} = 1$. We quantify the device loss thresholds for ballistic LOQC with k-qubit micro clusters as the initial resource, and pairwise fusion operations. Our results stress the importance of investigating efficient ways to directly generate entangled clusters of 3 or more qubits; as well as the need to investigate linear optical methods for simultaneous fusion of 3 or more qubits.

PACS numbers: 42.50.Ex, 03.67.Dd, 03.67.Lx, 42.50.Dv

The Knill-Laflamme-Milburn (KLM) model of quantum computing, popularly known as *Linear-optical quantum computing (LOQC)*, uses a single photon in one of two orthogonal (spatial, temporal or polarization) modes, i.e., $|10\rangle$ and $|01\rangle$ to encode a qubit, and uses passive linear optical interferometers and single-photon detectors to implement gates and measurements. Gates and measurements in LOQC are inherently probabilistic even if all the single-photon sources are ideal, and all the linear optics and detectors are lossless. Component losses further reduce the success probabilities of gates and measurements, which translate into astronomical requirements on devices for problems of practically-relevant size. Since the original KLM proposal—which was largely deemed unscalable due to the aforesaid reason, several improved proposals for LOQC have been proposed that use a combination of injecting separately-prepared ancilla photons, and using photon number resolving detectors.

Entangled k-qubit micro clusters can be stitched together using probabilistic m-qubit linear-optic fusion operations that succeed with probability λ—without any measurement-induced feedforward—into a giant connected component (GCC) of a random percolated instance of a target lattice G, if $\lambda > \lambda_c^{(k,m)}$. The threshold $\lambda_c^{(k,m)}$ depends upon the choice of G and the sequence of fusion steps. This GCC can then be renormalized into a square-grid cluster universal for measurement based quantum computing. With two-qubit fusion operations ($m = 2$), we give an explicit construction that shows $\lambda_c^{(3,2)} \leq 0.54$. This improves over a recently published threshold of 0.625 when 3-qubit (GHZ) states are used as the initial resource; a smaller threshold on λ implies a higher resilience to device losses. We also show that $\lambda_c^{(k,2)} \geq 1/(k-1)$ for all $k \geq 2$. With 3-qubit (GHZ) states as the initial resource, $\lambda_c^{(3,2)} \geq 0.5$, which implies that a fusion gate based on passive linear optics will not work (due to its 0.5 success-probability limit) and that one must use fusion gates boosted with injected single photons or 2-qubit entangled Bell states. Further, with 2-qubit (Bell) states as the initial resource, ballistic linear-optical quantum computing is practically impossible using pairwise fusion operations, since $\lambda_c^{(2,2)} = 1$. We quantify the device loss thresholds for ballistic LOQC with k-qubit micro clusters as the initial resource, and pairwise fusion operations. Our results stress the importance of investigating efficient ways to directly generate entangled clusters of 3 or more qubits; as well as the need to investigate linear optical methods for simultaneous fusion of 3 or more qubits.

MP, DRE, and SG acknowledge support from the DARPA seedling project *Scalable Engineering of Quantum Optical Information Processing Architectures* (SEQUOIA), under US Army contract number W31P4Q-15-C-0045. SG was also partially supported by an ONR-funded project on Optical Computing. MP and SG acknowledge extremely valuable discussions with Terry

Rudolph and Mercedes Gimeno-Segovia during their visit to Boston in April 2016.

[*] mpant@mit.edu

Scalable Engineering of Quantum Optical Information Processing Architectures (SEQUOIA) – final review

September 1, 2016

BBN and MIT

Raytheon
BBN Technologies

SEQUOIA team

- BBN
  - Saikat Guha (PI)
  - Hari Krovi
  - Jonathan Habif
  - Mohammad Soltani

- MIT
  - Dirk Englund
    - Mihir Pant (also at BBN)
    - Mikkel Heuck*
    - Nick Harris*
    - Mihika Prabhu*
  - Karl Berggren
    - Qingyuan Zhao
    - Francesco Bellei
    - Di Zhu

* not supported by DARPA

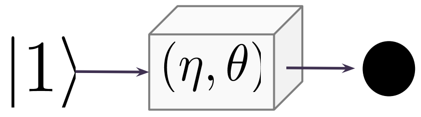
Outline

- **Theory summary**
  - Ballistic LOQC
    - trade-off between size of input clusters and loss tolerance
    - Minimum resource state: GHZ states
  - All-optical quantum repeater
    - Second-generation
      - Tree code
      - GHZ sources
    - Third-generation scheme
      - Parity code
      - GHZ source
  - In-line NL and Ising
- **Quantum device engineering**
  - How to generate GHZ resource states?
    - Heralded 6-wave mixing
    - On-demand generation with QND measurements
  - Quantum programmable processor
    - Green machine implementation
    - Prospect of realizing “boosted” gates: single-photon injection / mode-matching
  - Optical quantum computing with in-line non-linearities
    - Spectral encoding of dual rail qubits in coupled cavities
    - Ising model implementation
  - Comparative device study
- **SNSPD**
  - Scalable readout
  - Thermal compatibility with QPP
- **LOQC program vision**

LOQC: some building blocks

single (dual rail) qubit

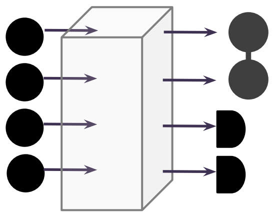
beam-splitter



$$\sqrt{\eta}e^{i\theta}|10\rangle+\sqrt{1-\eta}|01\rangle$$

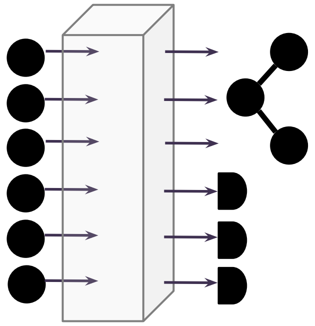
single photon

2-qubit entangled
Bell state

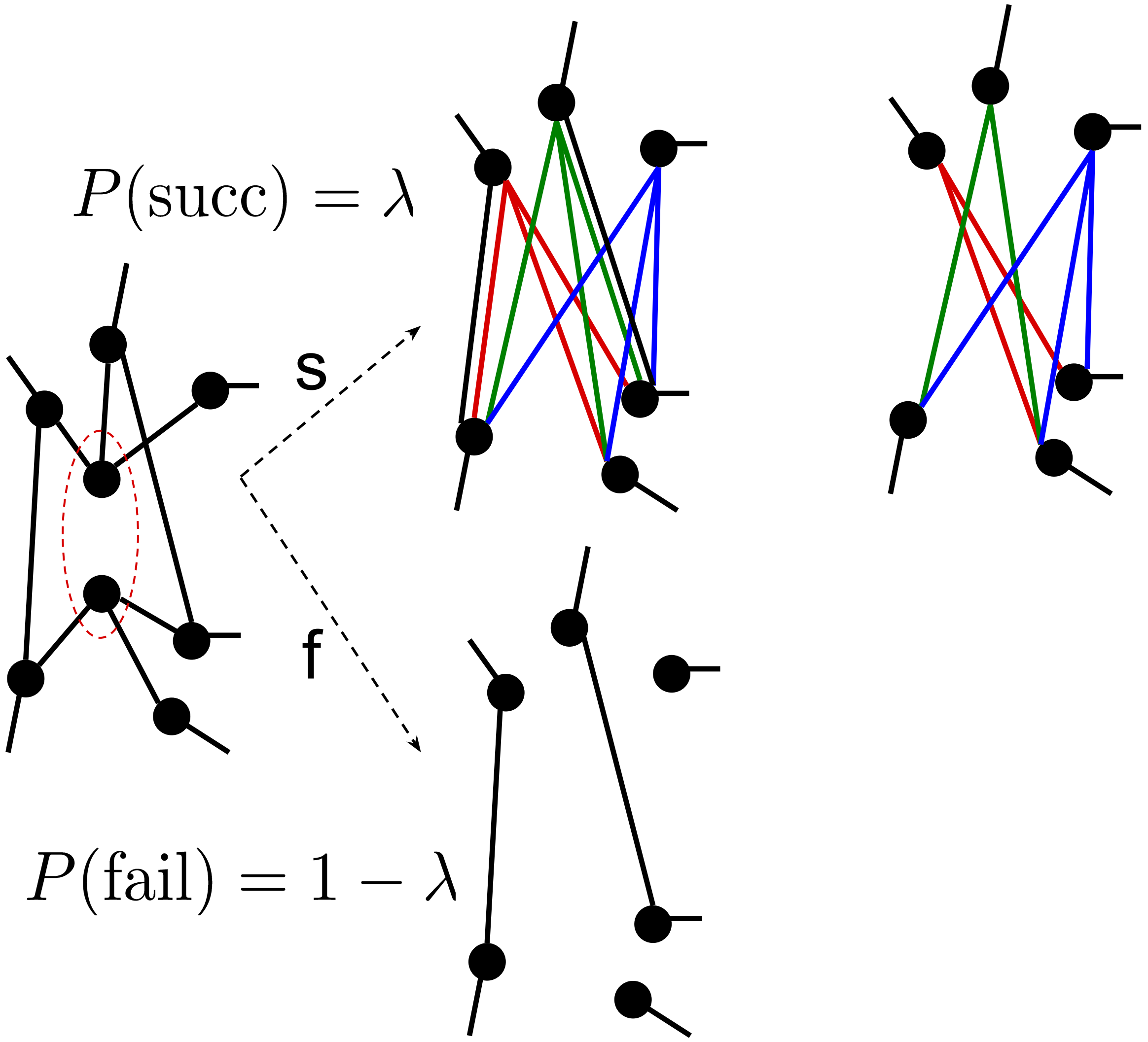


$$p_s=\frac{3}{16}$$

3-qubit entangled
GHZ state



$$p_s=\frac{1}{32}$$



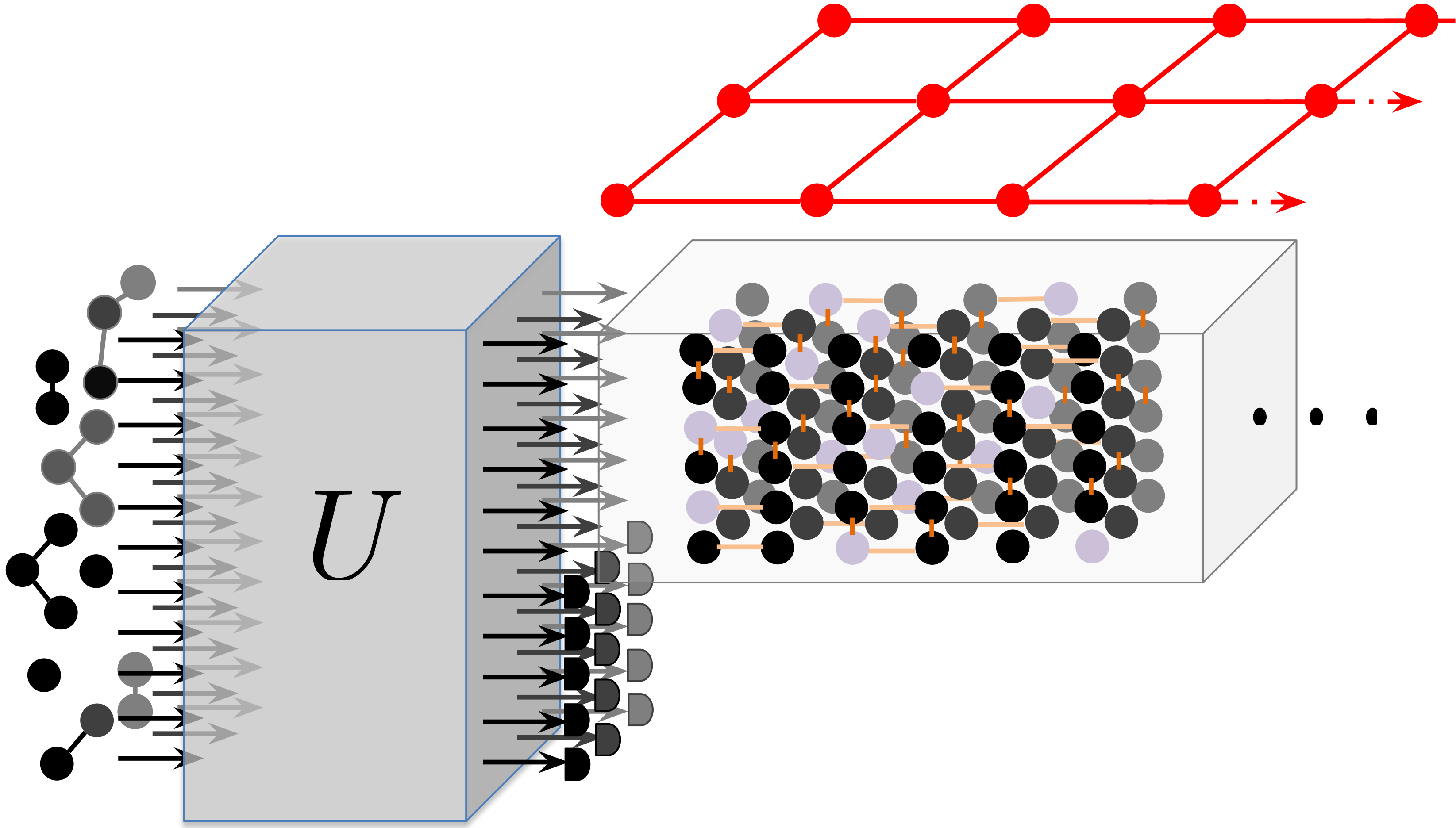
λ = 0.5 (max with linear optics)
λ = 0.75 (linear optics with two injected single photons)
λ = 1-1/2^N (2^N-2 injected 2-qubit Bell pairs)

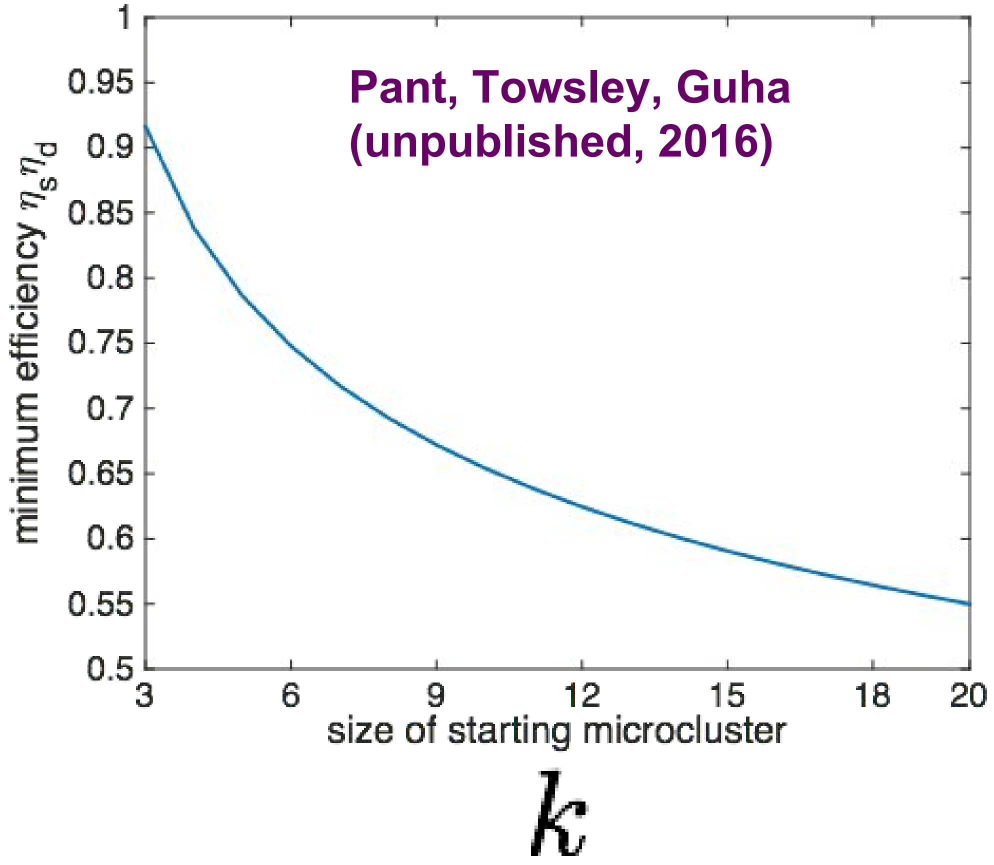
(detector and/or sources losses reduce all the above numbers)

Any graph state can be put together with GHZ states and 2-qubit Type-II Fusion

LOQC (KLM and beyond): single photons, linear optics, feedforward, and single photon detection

Ballistic QC with microclusters

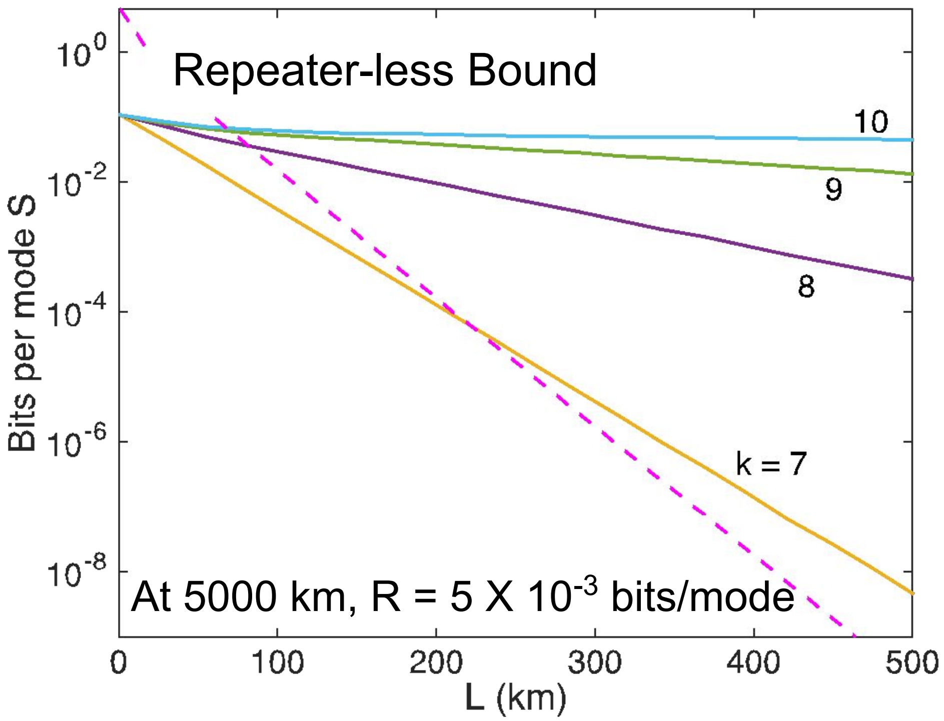



Pant, Towsley, Guha (unpublished, 2016)

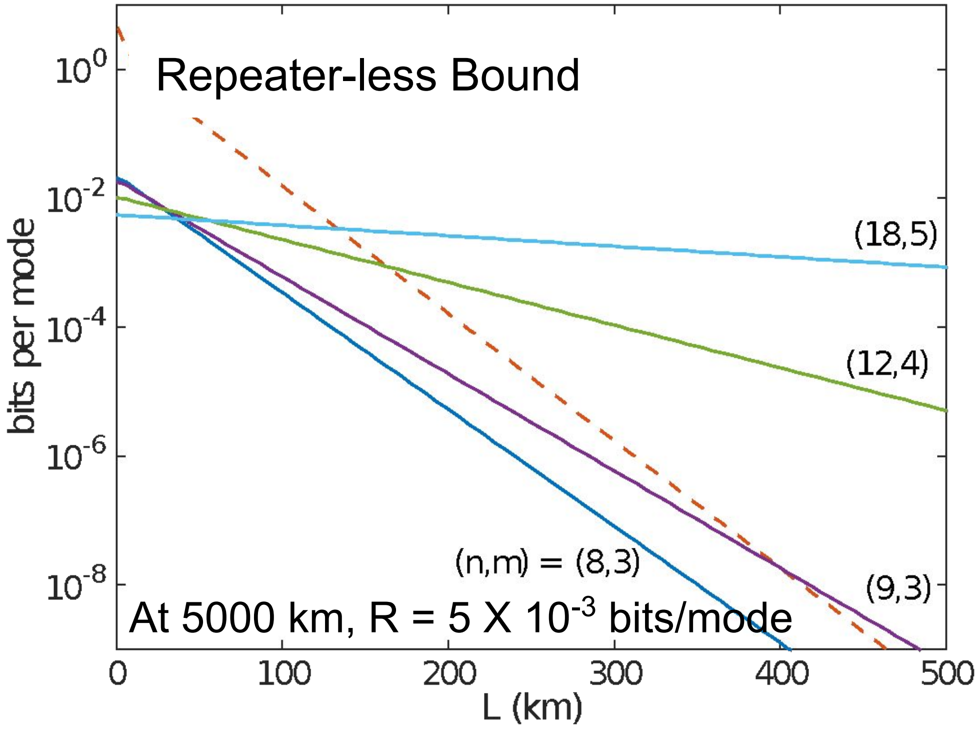
Goal: create a resource that is sufficient for universal QC in a loss tolerant way using minimum possible feedforward

- k = 1 (Boson sampling), output cluster is disconnected: not a good enough resource for universal QC
- k = 2 (Bell pair initial resource), output barely percolates if all efficiencies are 100% (no loss tolerance)
- k = 3 (3-photon GHZ is initial resource), then ballistic QC is possible
  - 3D-diamond (Rudolph *et al.*); λ_c = 62.5%; loss tolerance: $\eta_s\eta_d$ > **96.2%**
  - (10,3)-b lattice (our method); λ_c = 54%; loss tolerance: $\eta_s\eta_d$ > **93.4%**
  - Best possible lattice (converse proof / Bethe lattice); λ_c = 50%; max possible loss tolerance: **91.6%**
- **Sources of >= 3-qubit microclusters needed if we want to avoid feed-forward, switching, and associated losses**

All optical repeaters



At 5000 km, R = 5 X 10^{-3} bits/mode



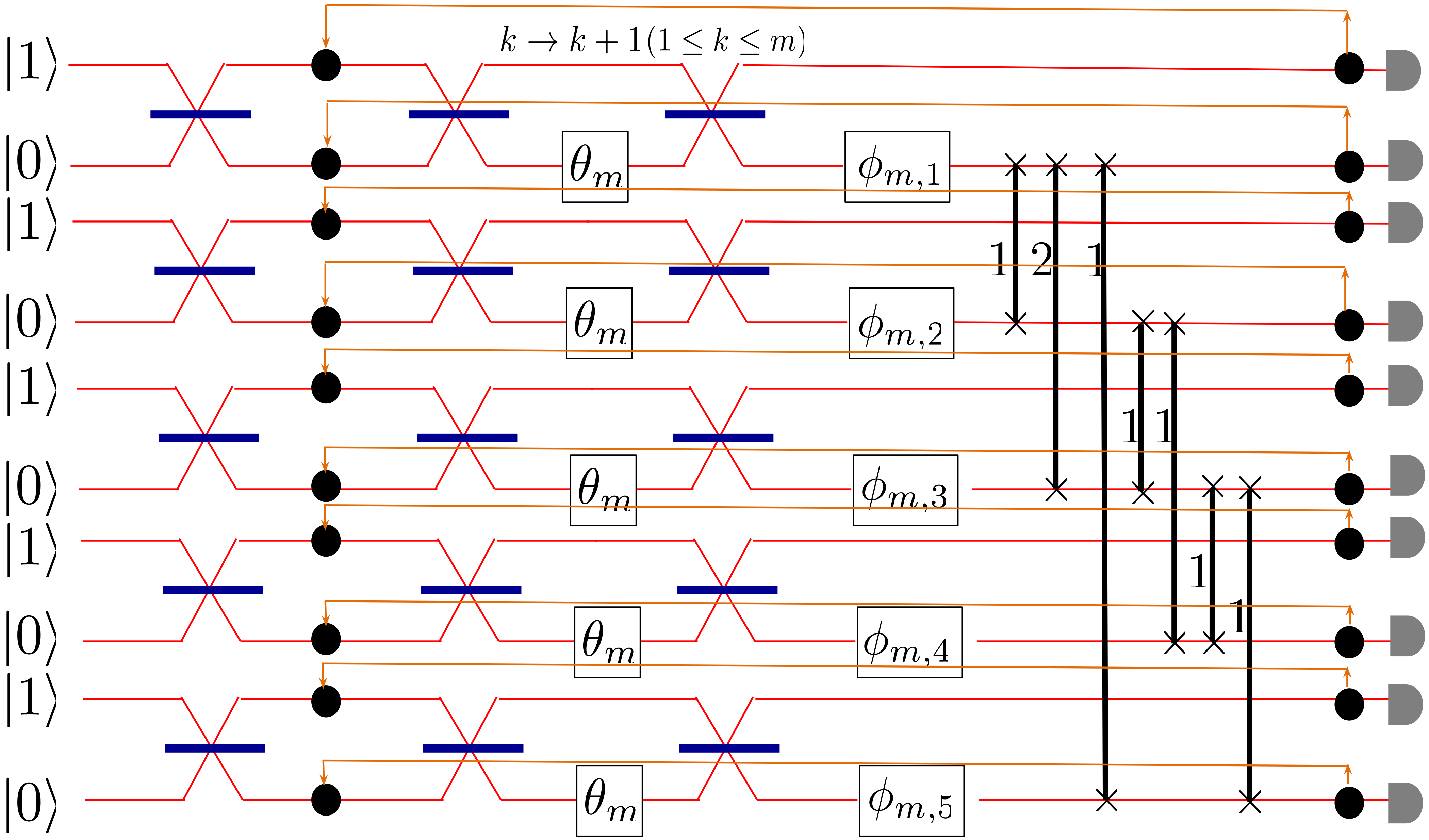
At 5000 km, R = 5 X 10^{-3} bits/mode

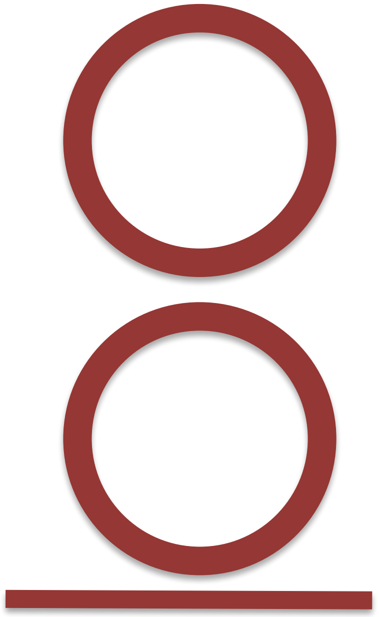
k	size of state	# of single-photon-sources	# on-demand GHZ states
7	113	3 M	15 k
8	237	10 M	50 k
9	489	36 M	180 k
10	993	120 M	600 k

(m,n)	size of state	# of single-photon-sources	# on-demand GHZ states
(8,3)	48	200k	1k
(9,3)	54	700k	3.5k
(12,4)	96	2M	10k
(18,5)	180	4.4M	22k

- 3rd gen + QPC > 2nd gen + tree code by 10x in #sources/node. (10^5 x from Lo et al.)
- Availability of 3-photon GHZ sources reduces the #sources by > 2 orders of magnitude
- Both can beat repeaterless ideal QKD protocol, even with losses (in all devices, coupling, detectors). Mode mismatch, g(2) and excess noise not included; initial network results
- Systematic study of QEC for optics-errors: loss, indistinguishability, noise, g(2), spectral purity, etc.

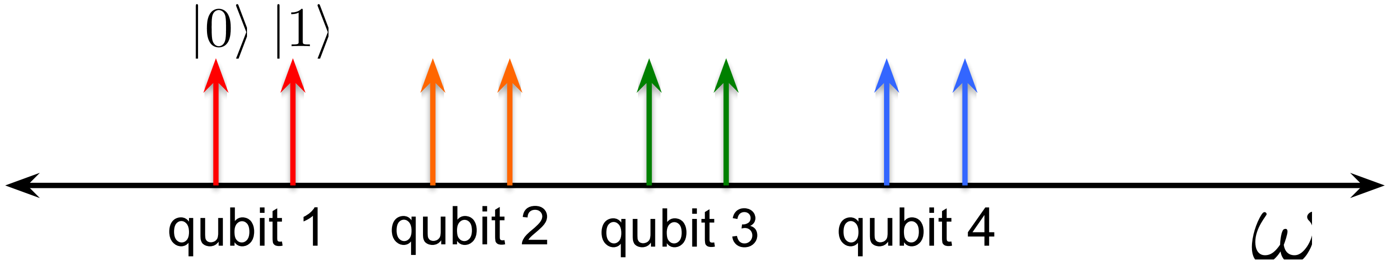
In-line non-linearities - Optical Ising solver





$$\theta_m = \frac{T}{m}\left[1 - \frac{k}{m}\right]\pi \qquad \phi_{m,i} = B_i \frac{Tk\pi}{m^2} \qquad \chi_{ij} = J_{ij}\frac{Tk\pi}{m^2}$$

Krovi, Guha, Pant, Englund (unpublished, 2016)

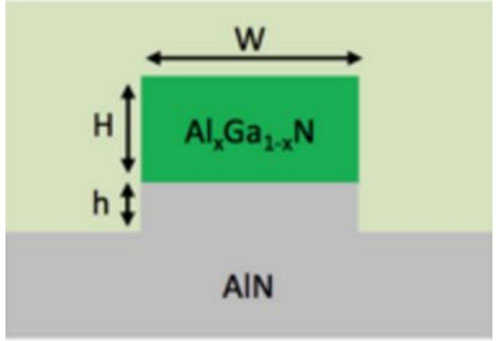


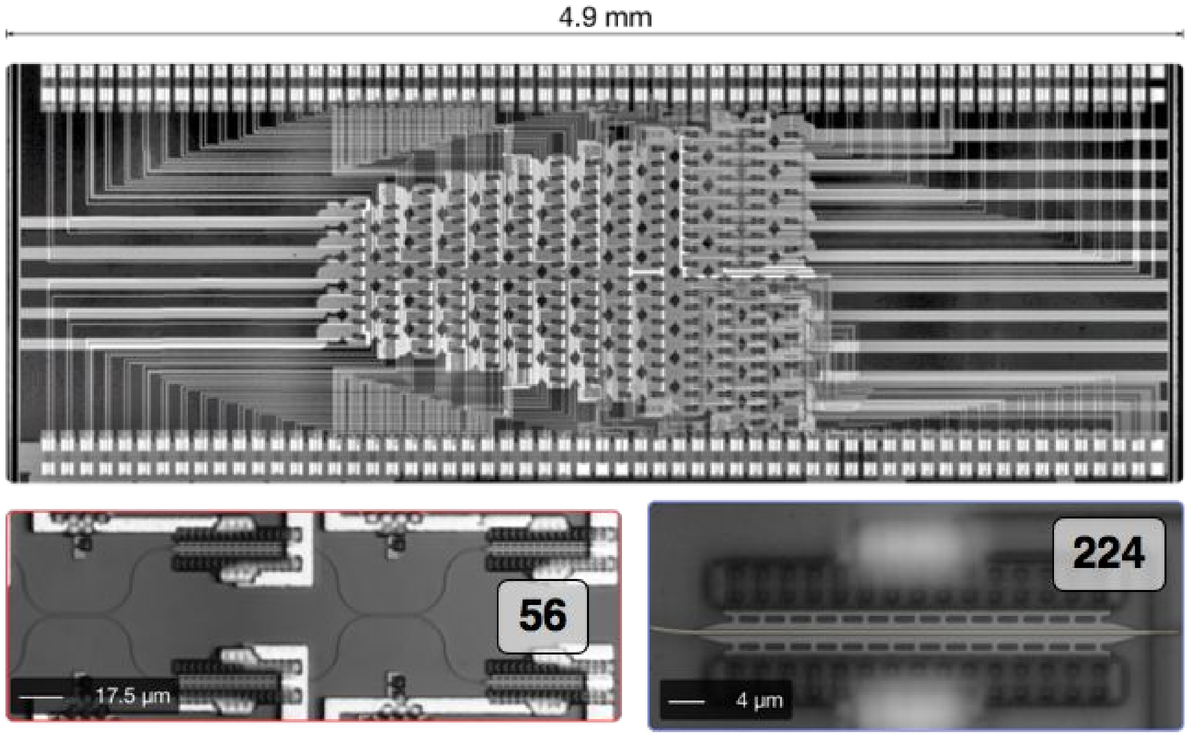
SEQUOIA theory work: summary

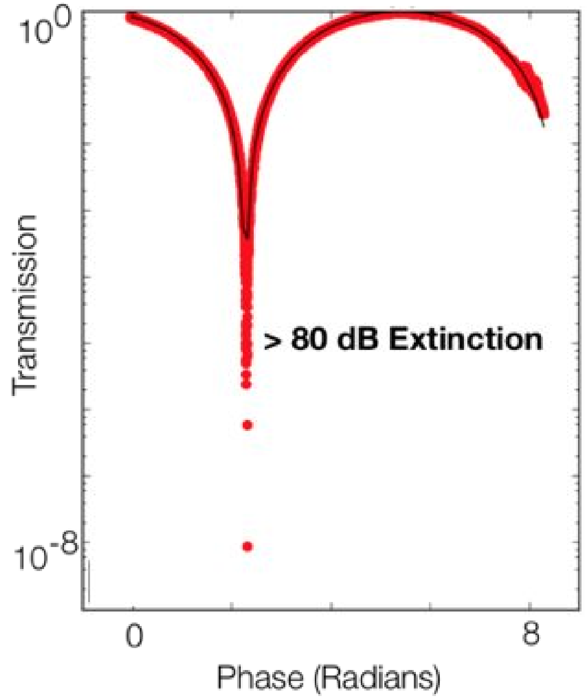
- General facts we have learnt about LOQC
  - Tradeoff: offline (photons/ent. states) vs. inline (NL) resource. Inline often hard
  - LOQC with **offline** photons/entanglement (heralded / probabilistic is OK):
    - Offline states >= 3-qubit microclusters, feedforward need drastically reduces: “Ballistic” LOQC / relationship to BosonSamp
    - Larger microclusters, higher loss tolerance; fewer sources (of such microclusters)
  - Hybrid methods:
    - Offline and inline can be used simultaneously to trade some benefits of both
    - CV cluster states can be used for universal QC with PNR and homodyne
  - LOQC with **inline**: Special purpose processor / quantum annealing, Ising model
- All-optical repeaters: special-purpose LOQC (**offline** resources)
  - 3rd gen + QPC > 2nd gen + tree code by 10x in #sources/node. (10^5 x from Lo *et al.*)
  - Availability of 3-photon GHZ sources reduces the #sources by > 2 OoM
  - Both can beat repeaterless ideal QKD protocol, even with losses (in all devices, coupling, detectors). Mode mismatch, g(2) and excess noise not included; initial network results
- Challenges stemming by theory work in SEQUOIA
  - Direct generation of microclusters (>= 3 qubits) with high fidelity very important
  - In-line (e.g., cross-Kerr) non-linearities, even if small, can be very useful
  - Systematic study of QEC for optics-errors: loss, indist, noise, g(2), spectral purity, etc.

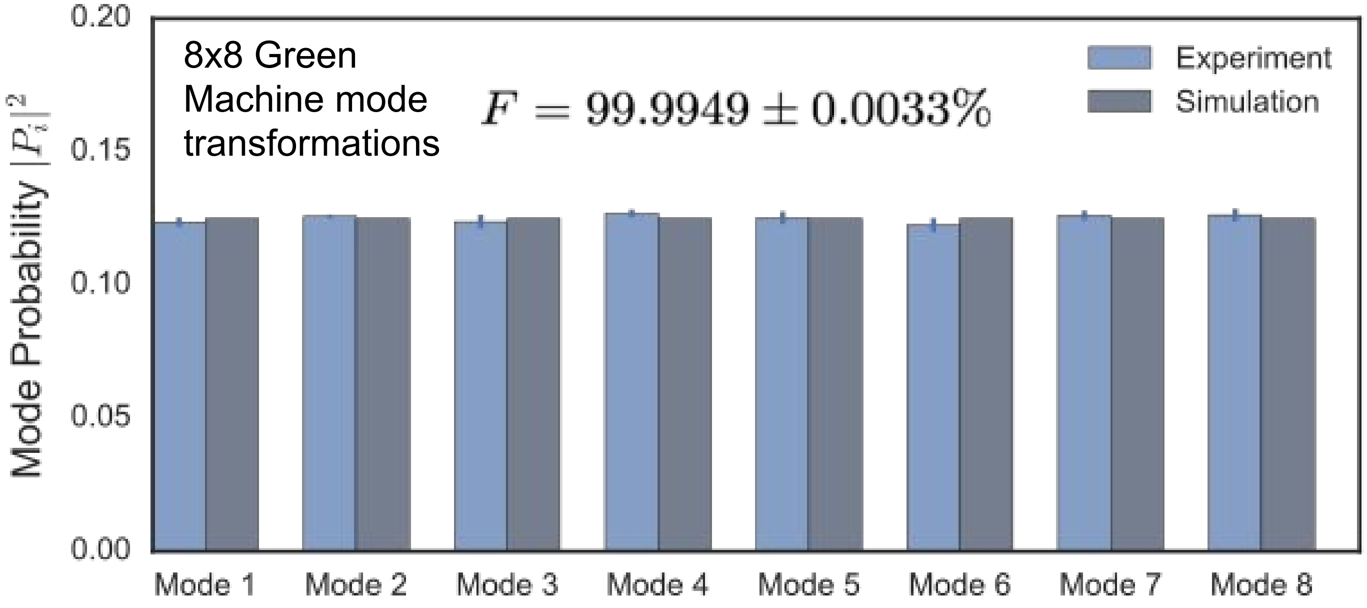
Programmable linear optics transformations

- Single-qubit gate infidelities < 10^{-7}
- PIC demonstrated with up to 26 individually connected output modes
- III-Nitride platform [Soltani, Soref, Palacios, Englund]

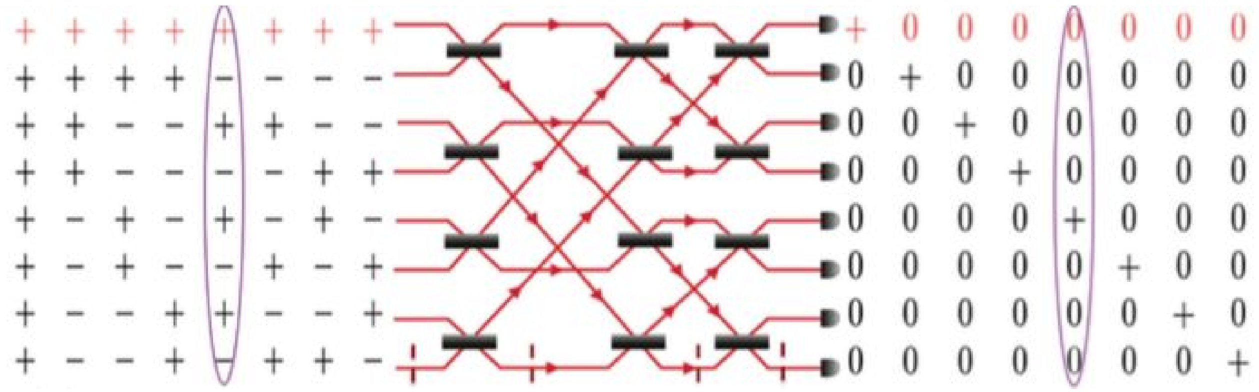







8x8 Green Machine mode transformations

$F = 99.9949 \pm 0.0033\%$



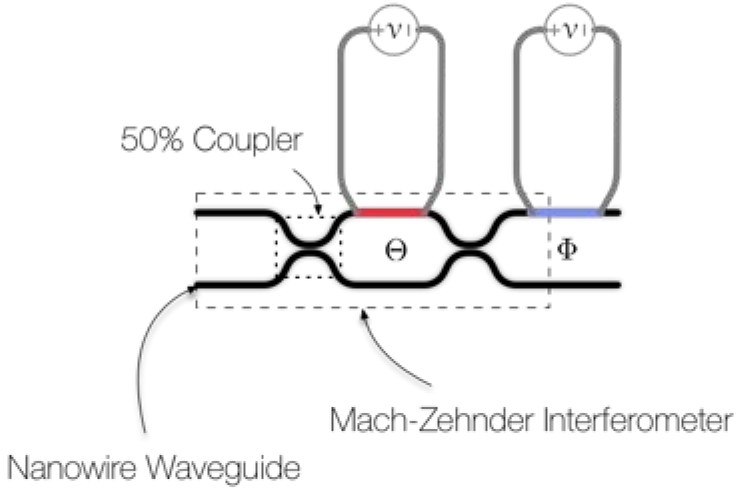
+	+	+	+	+	+	+	+
+	+	+	+	−	−	−	−
+	+	−	−	+	+	−	−
+	+	−	−	−	−	+	+
+	−	+	−	+	−	+	−
+	−	+	−	−	+	−	+
+	−	−	+	+	−	−	+
+	−	−	+	−	+	+	−

+	0	0	0	0	0	0	0
0	+	0	0	0	0	0	0
0	0	+	0	0	0	0	0
0	0	0	+	0	0	0	0
0	0	0	0	+	0	0	0
0	0	0	0	0	+	0	0
0	0	0	0	0	0	+	0
0	0	0	0	0	0	0	+

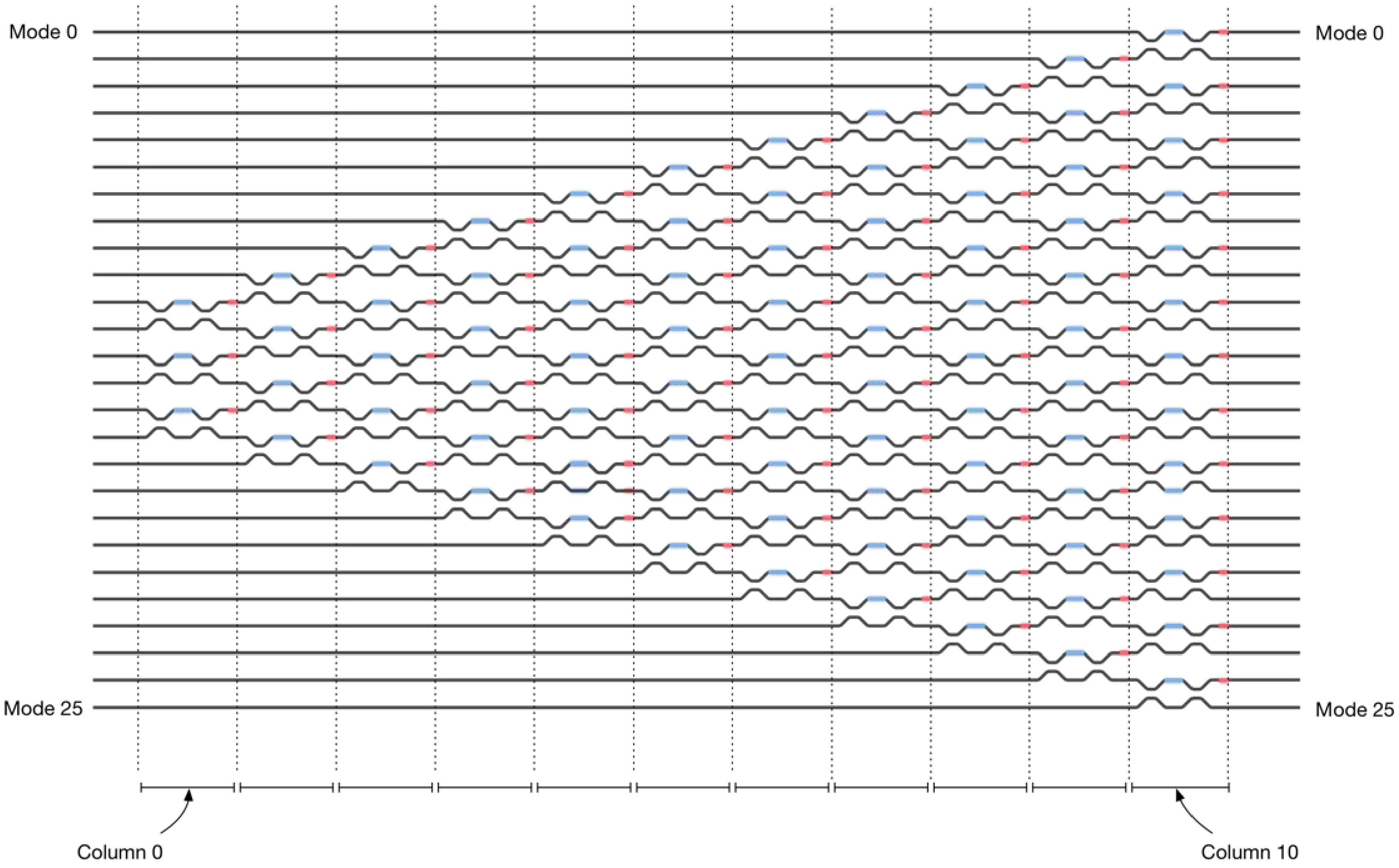
Programmable Nanophotonic Processor

- Reck and Zeilinger, PRL 73 (1994): any linear optics unitary can be produced using 4-port beamsplitters

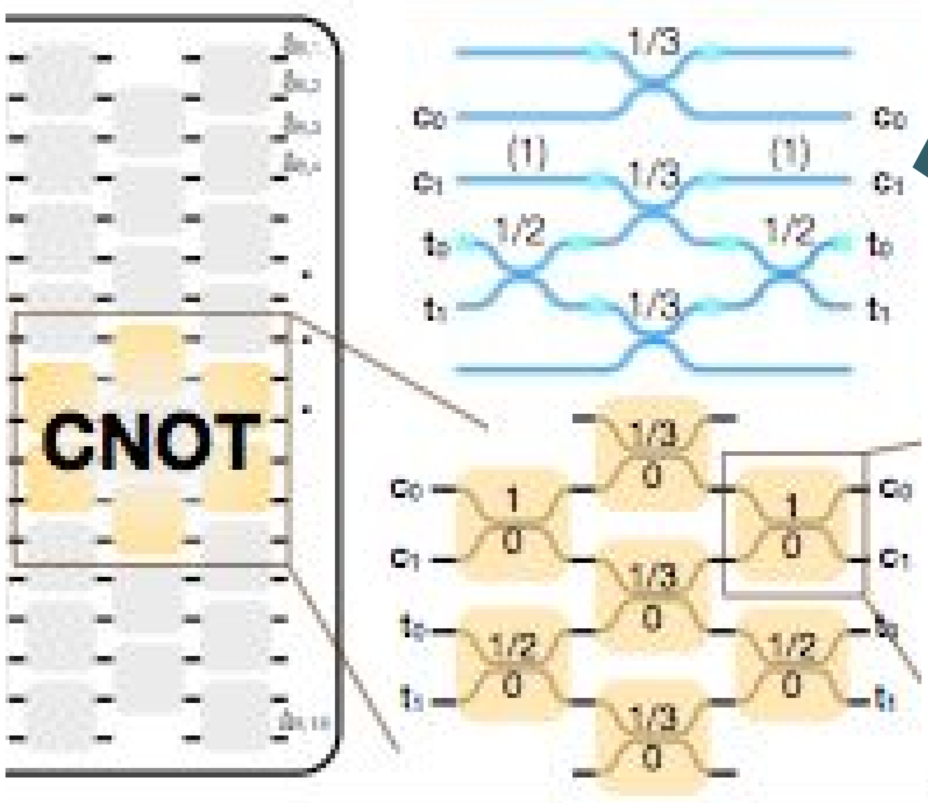
$$\tau \simeq 10\mu s$$



$$\hat{U} = \begin{bmatrix} e^{i\Phi}\sin(\Theta) & e^{i\Phi}\cos(\Theta) \\ \cos(\Theta) & -\sin(\Theta) \end{bmatrix}$$

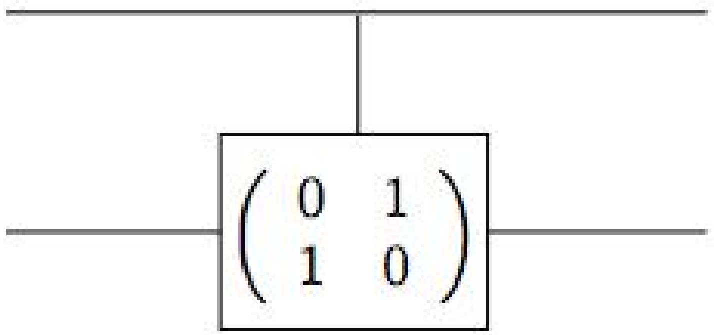


Perfect optics from imperfect components

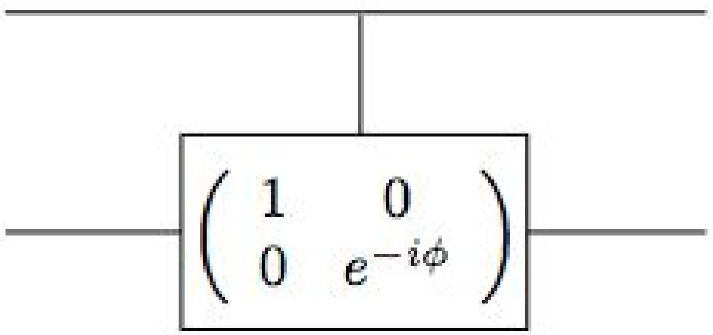


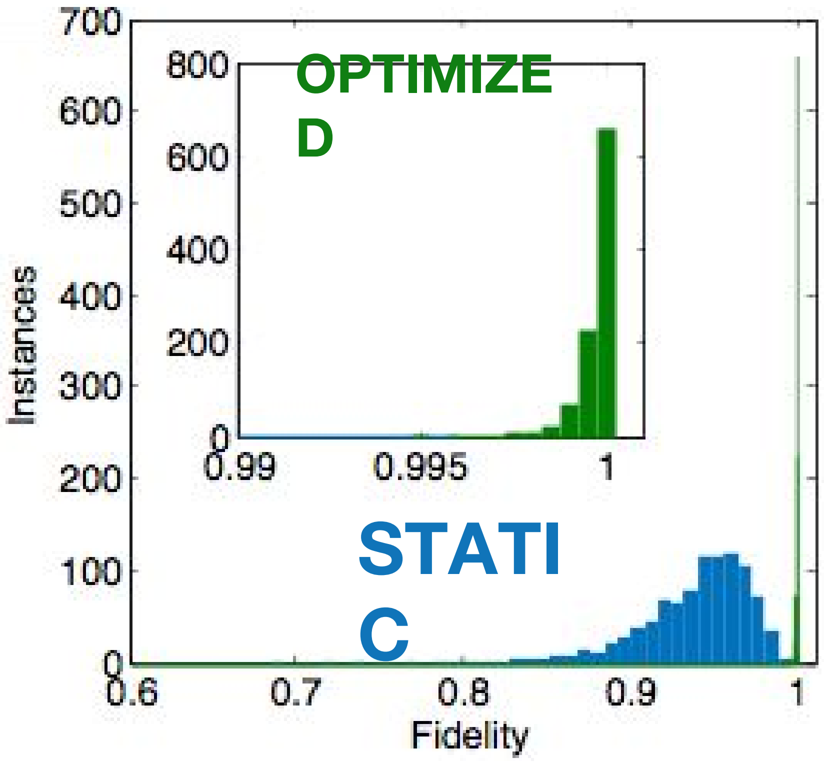
dual rail encoding

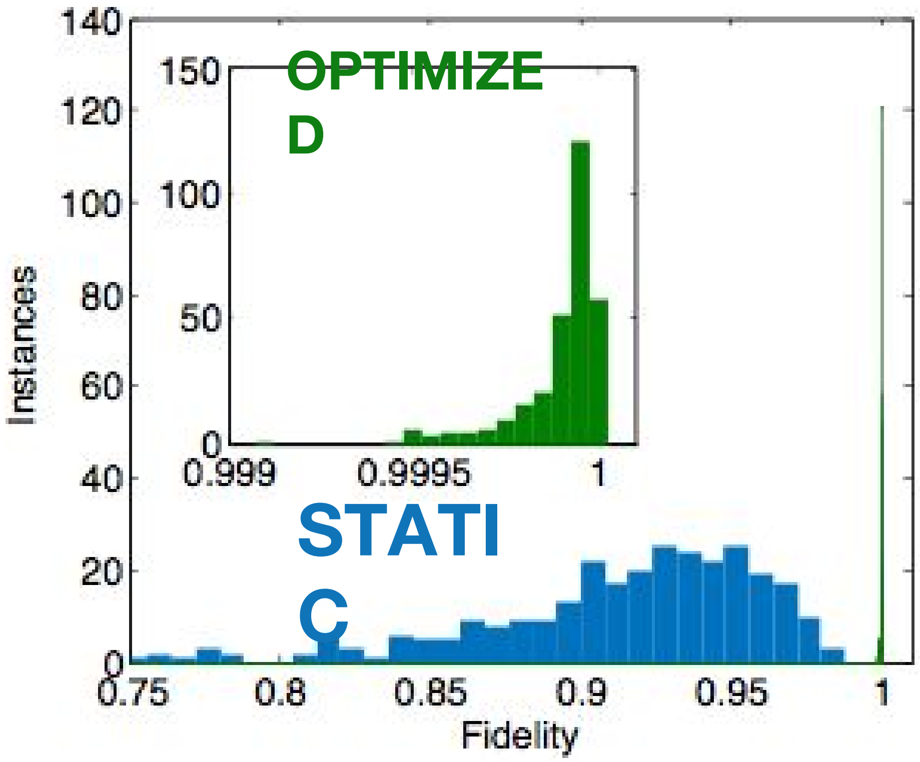
CNOT



CPHASE



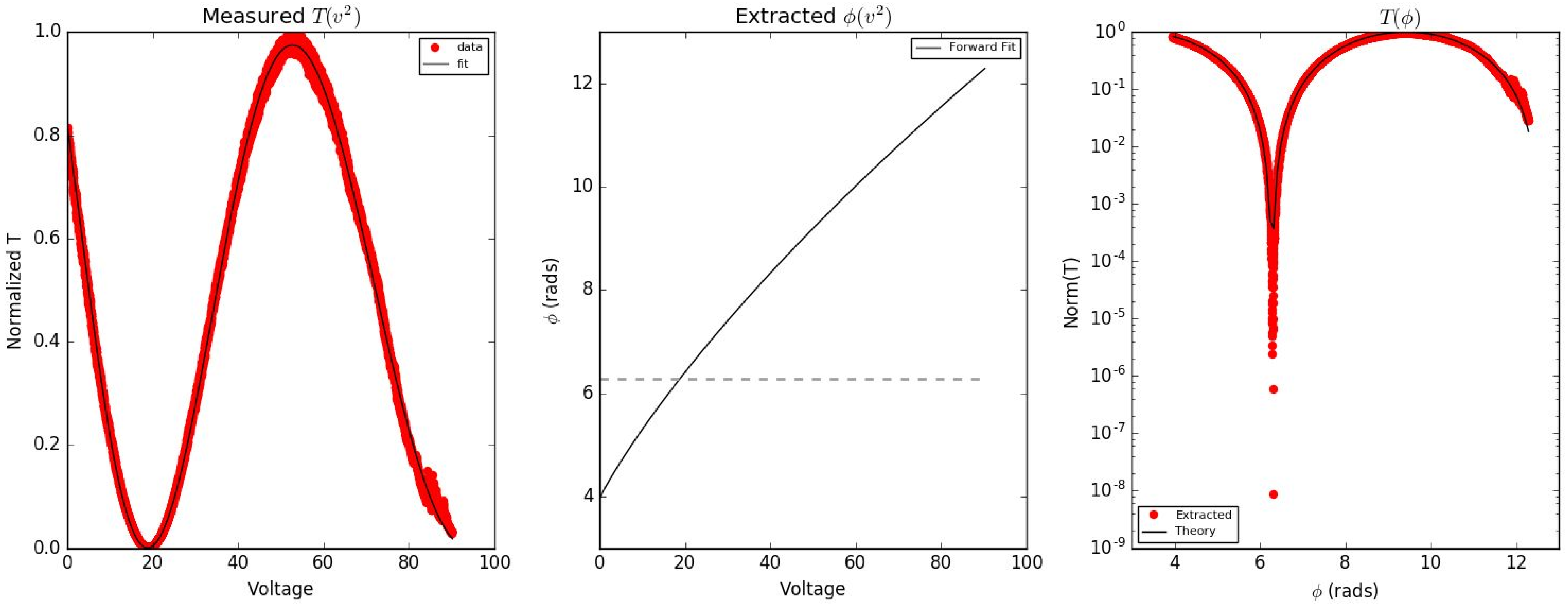




Assume
r=50%+- 2.1%

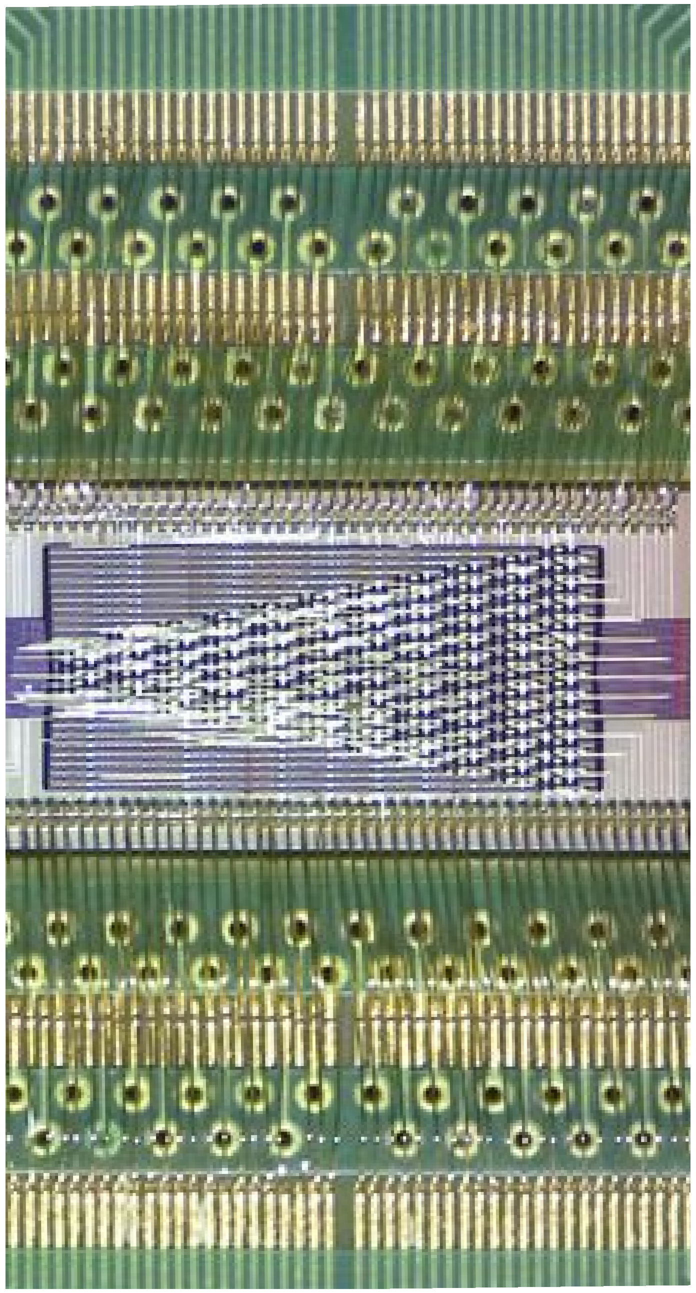
J. Mower*, N. C. Harris*, G. R. Steinbrecher*, Y. Lahini, D. Englund, to appear in Phys Rev A. *equal contributors

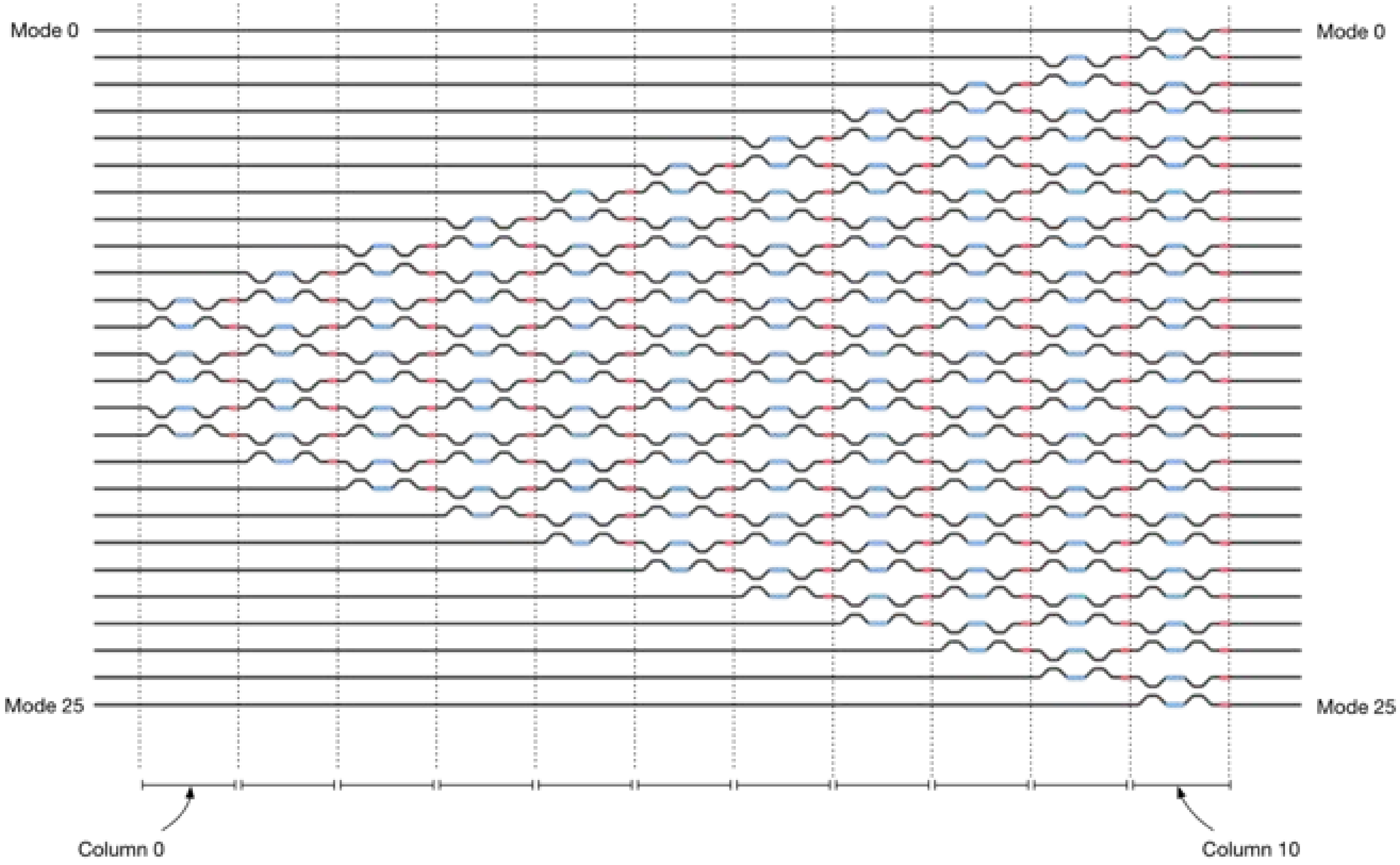
Excellent single-qubit gate fidelity



3rd Generation PNP

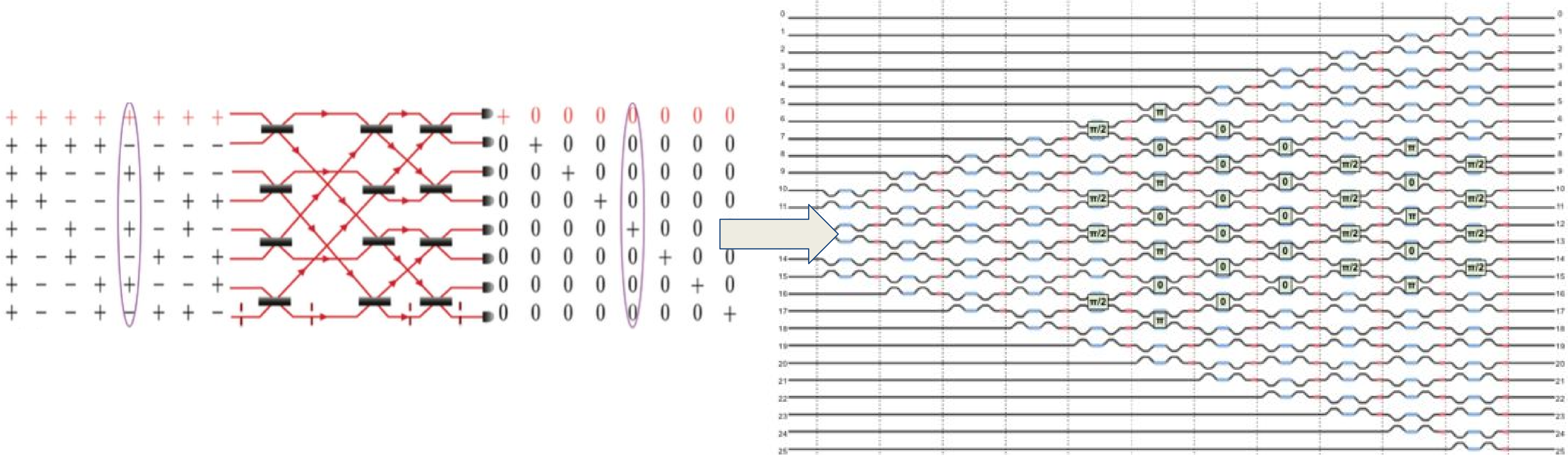
88 Interferometers, 26 individually connected output modes

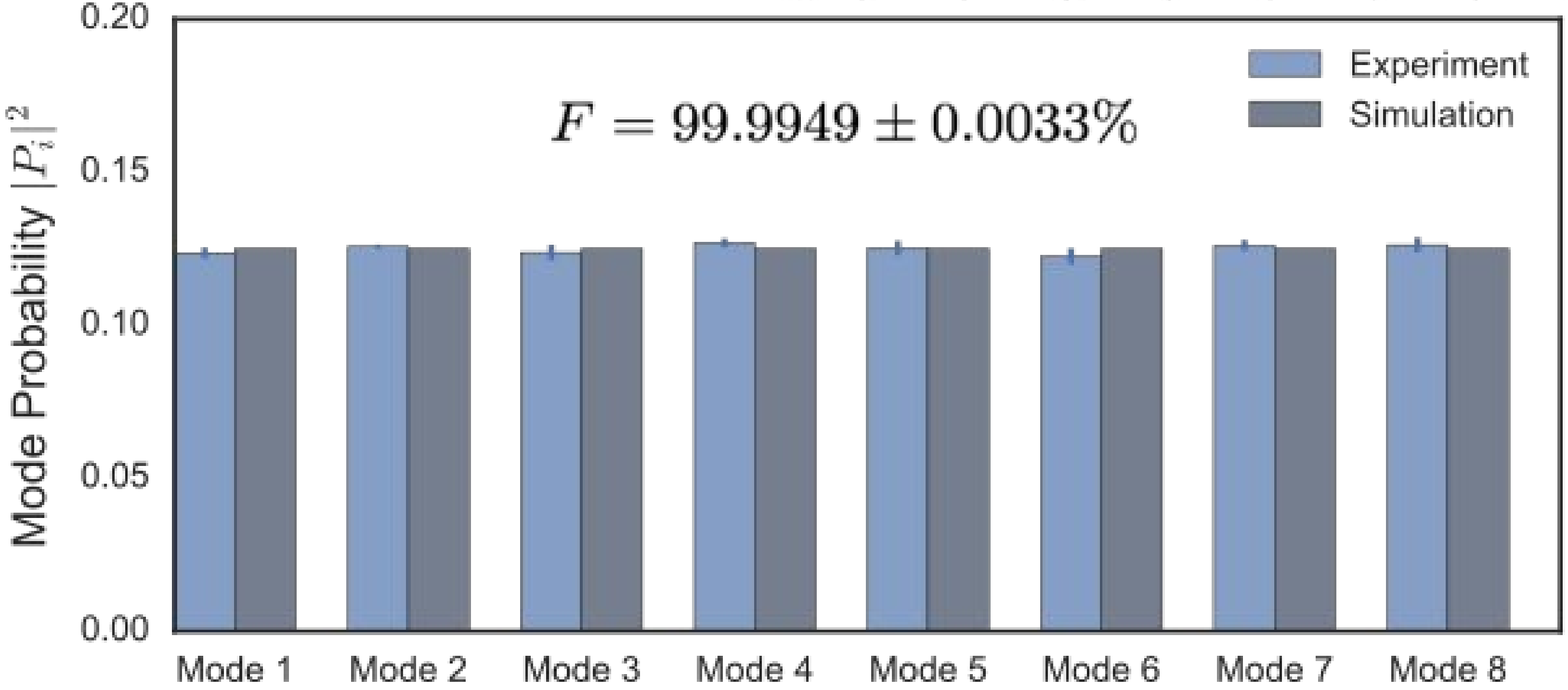




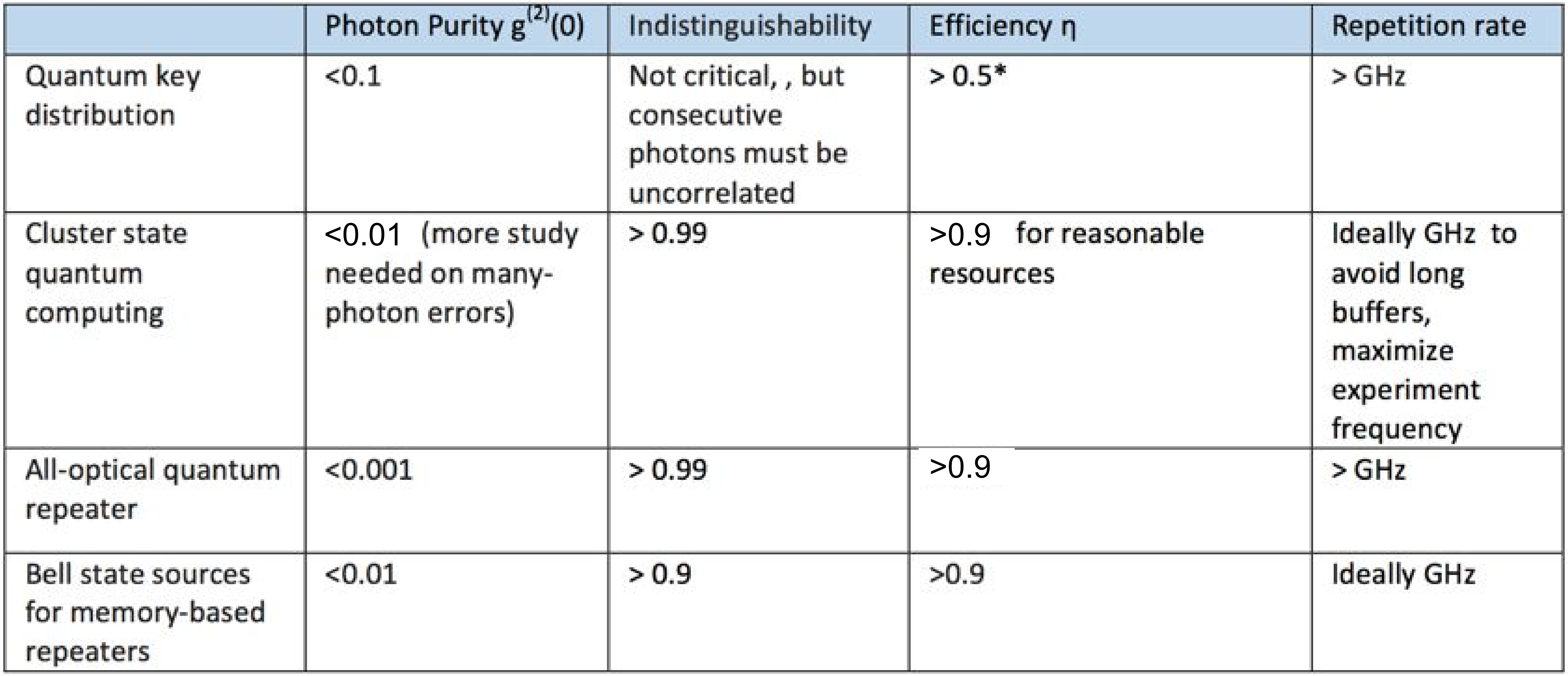
PNP Application: 8x8 Green machine

Operation for all 8 Hadamard code words





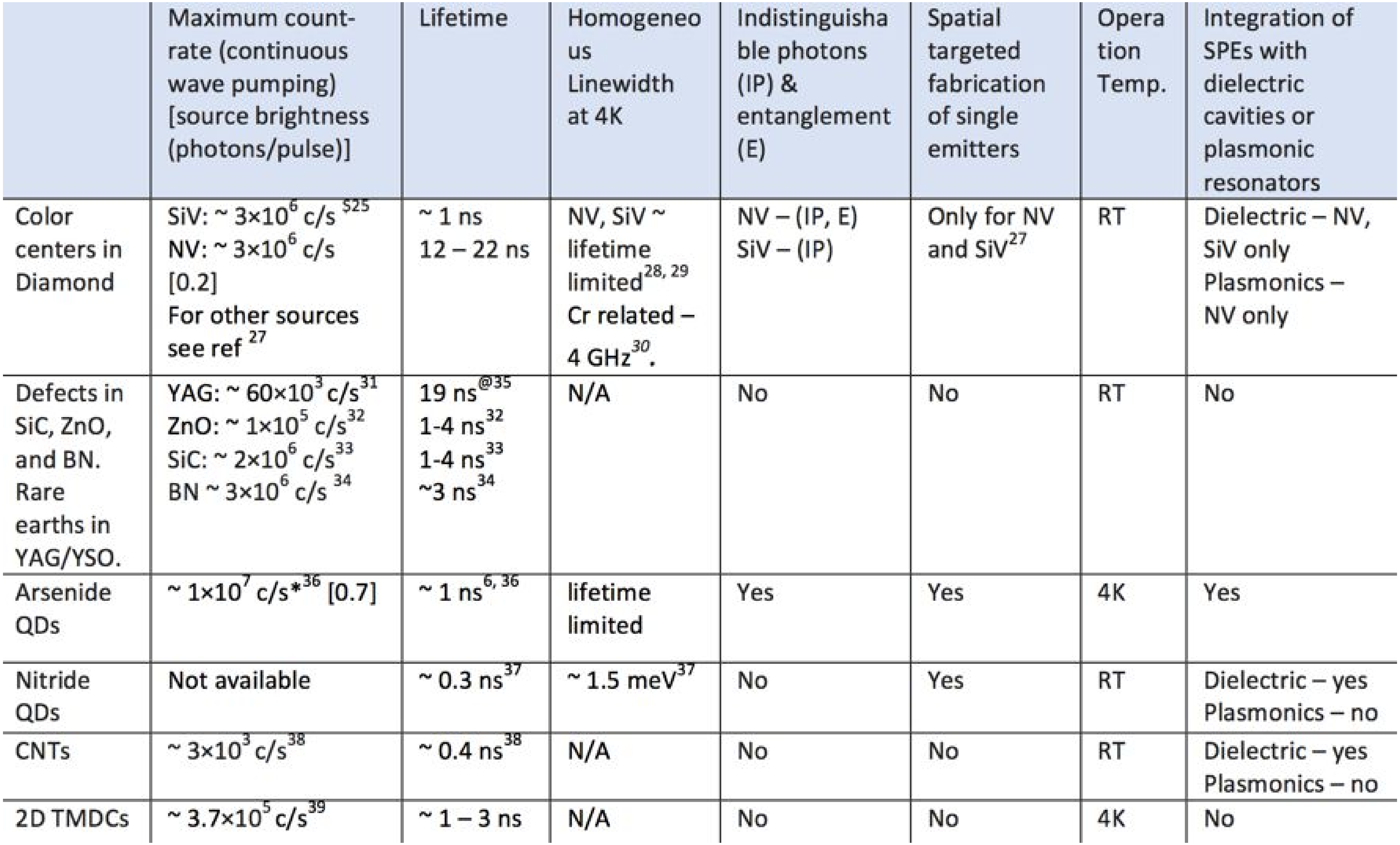
Light sources



	Photon Purity $g^{(2)}(0)$	Indistinguishability	Efficiency η	Repetition rate
Quantum key distribution	<0.1	Not critical, , but consecutive photons must be uncorrelated	> 0.5*	> GHz
Cluster state quantum computing	<0.01 (more study needed on many-photon errors)	> 0.99	>0.9 for reasonable resources	Ideally GHz to avoid long buffers, maximize experiment frequency
All-optical quantum repeater	<0.001	> 0.99	>0.9	> GHz
Bell state sources for memory-based repeaters	<0.01	> 0.9	>0.9	Ideally GHz

- On-Demand Single Photon emission based on quantum feedback control of a microcavity (manuscript to be submitted Sept 2016) [Heuck, Pant, Englund]
- 3-photon GHZ source based on 6-wave mixing (manuscript in preparation) [Pant, Soltani, Englund, Guha]
- On-demand GHZ source based on QND and dynamic cavity control (manuscript in preparation) [Pant, Guha, Englund]

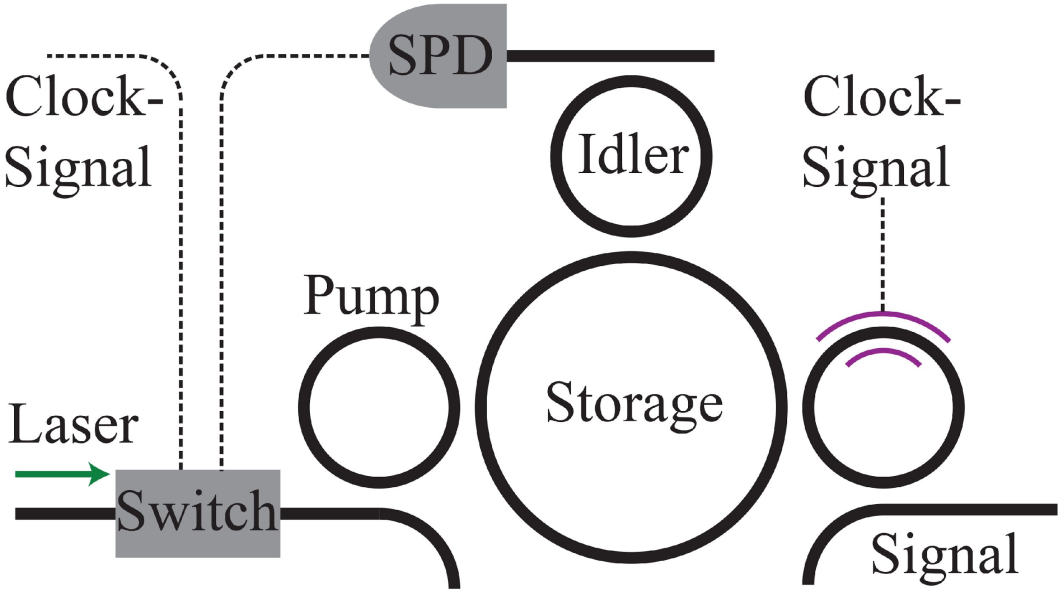
Light sources



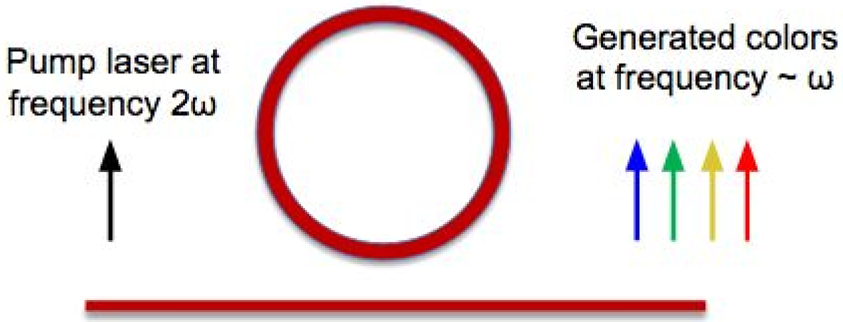
	Maximum count-rate (continuous wave pumping) [source brightness (photons/pulse)]	Lifetime	Homogeneous Linewidth at 4K	Indistinguishable photons (IP) & entanglement (E)	Spatial targeted fabrication of single emitters	Operation Temp.	Integration of SPEs with dielectric cavities or plasmonic resonators
Color centers in Diamond	SiV: ~ 3×10^{6} c/s [S25] NV: ~ 3×10^{6} c/s [0.2] For other sources see ref [27]	~ 1 ns 12 – 22 ns	NV, SiV ~ lifetime limited[28, 29] Cr related – 4 GHz[30].	NV – (IP, E) SiV – (IP)	Only for NV and SiV[27]	RT	Dielectric – NV, SiV only Plasmonics – NV only
Defects in SiC, ZnO, and BN. Rare earths in YAG/YSO.	YAG: ~ 60×10^{3} c/s[31] ZnO: ~ 1×10^{5} c/s[32] SiC: ~ 2×10^{6} c/s[33] BN ~ 3×10^{6} c/s [34]	19 ns[@35] 1-4 ns[32] 1-4 ns[33] ~3 ns[34]	N/A	No	No	RT	No
Arsenide QDs	~ 1×10^{7} c/s*[36] [0.7]	~ 1 ns[6, 36]	lifetime limited	Yes	Yes	4K	Yes
Nitride QDs	Not available	~ 0.3 ns[37]	~ 1.5 meV[37]	No	Yes	RT	Dielectric – yes Plasmonics – no
CNTs	~ 3×10^{3} c/s[38]	~ 0.4 ns[38]	N/A	No	No	RT	Dielectric – yes Plasmonics – no
2D TMDCs	~ 3.7×10^{5} c/s[39]	~ 1 – 3 ns	N/A	No	No	4K	No

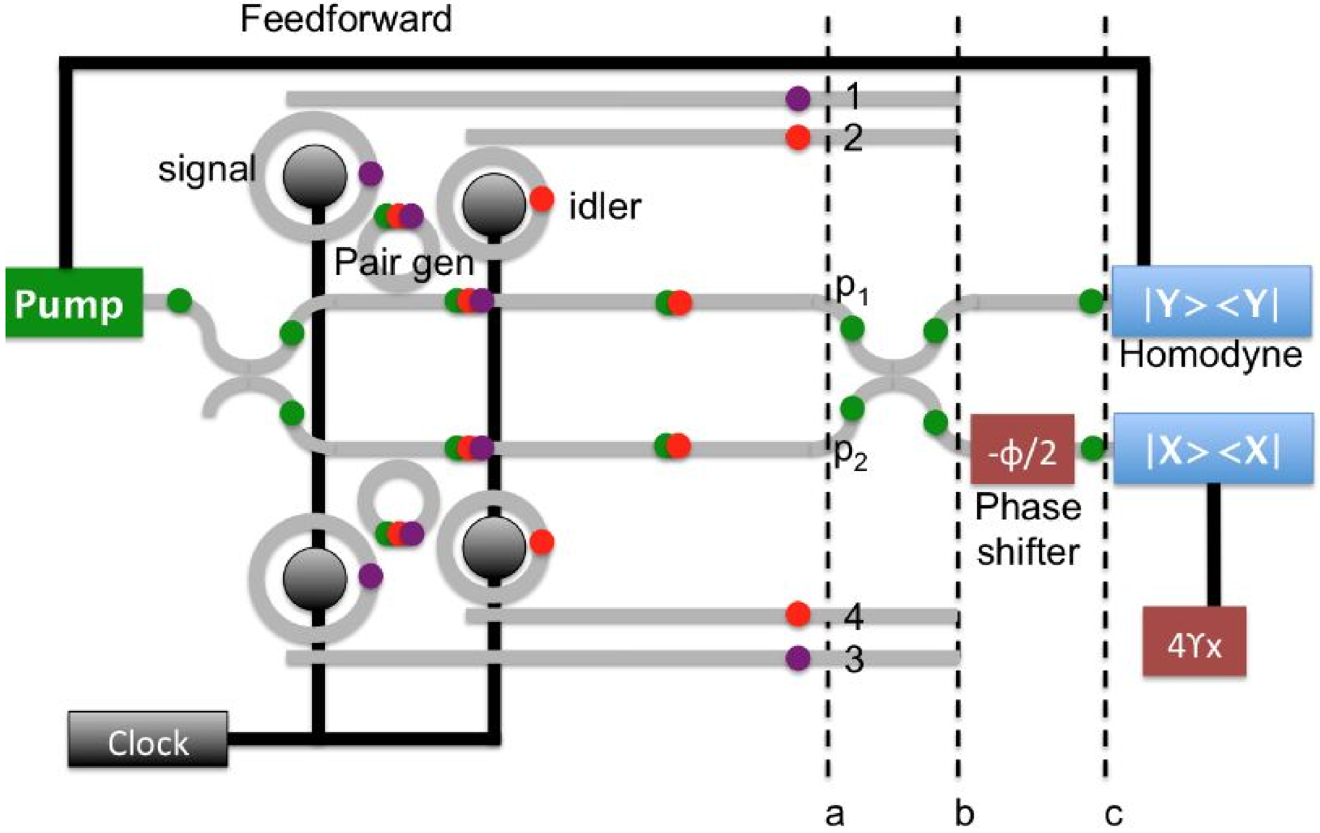
A source for scalable photonic QIP?

Can we develop a source satisfying the requirements of LOQC? We investigated three promising architectures:



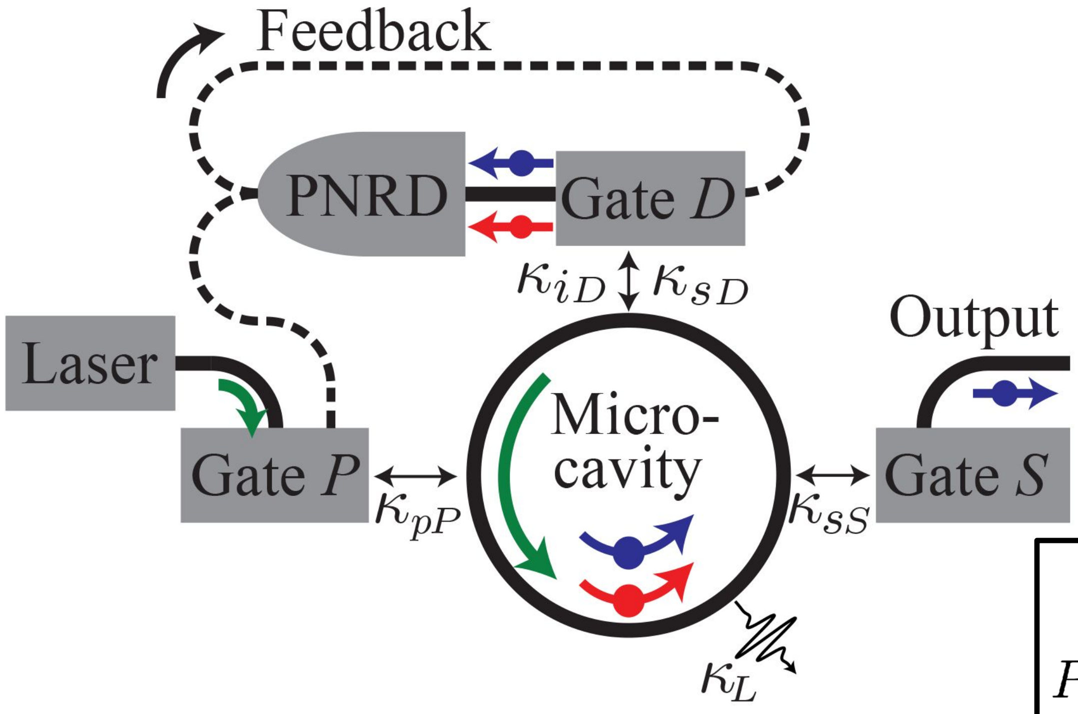
eff> 98% with spectral multiplexing, assuming good enough detectors (>99.5%)





- On-Demand Single Photon emission based on quantum feedback control of a microcavity (manuscript to be submitted Sept 2016) [Heuck, Pant, Englund]
- 3-photon GHZ source based on 6-wave mixing (manuscript in preparation) [Pant, Soltani, Englund, Guha]
- On-demand GHZ source based on QND and dynamic cavity control (manuscript in preparation) [Pant, Guha, Englund]

How to build a sufficient source?



Protocol

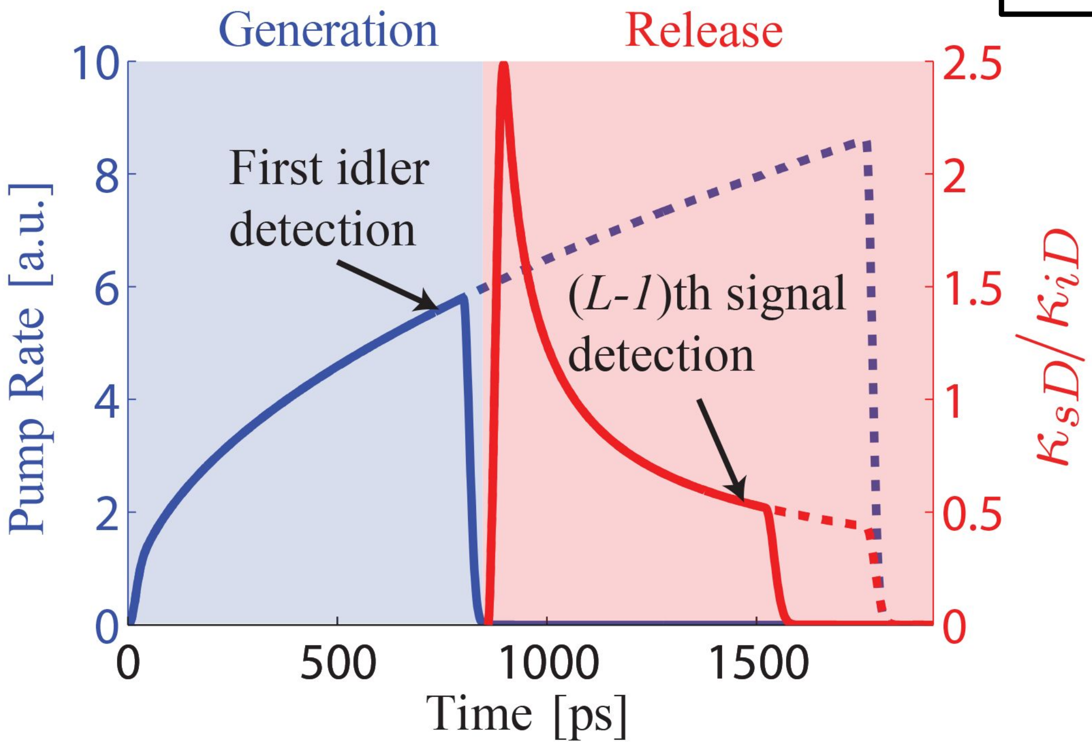
Generation

- Pump laser is turned off at the first idler detection.
- A total of n_A pairs are created and L idler photons are detected.

Release

- Coupling, κ_{sD}, is turned off at the (L-1)th signal detection.
- A total of N signal photons are detected.

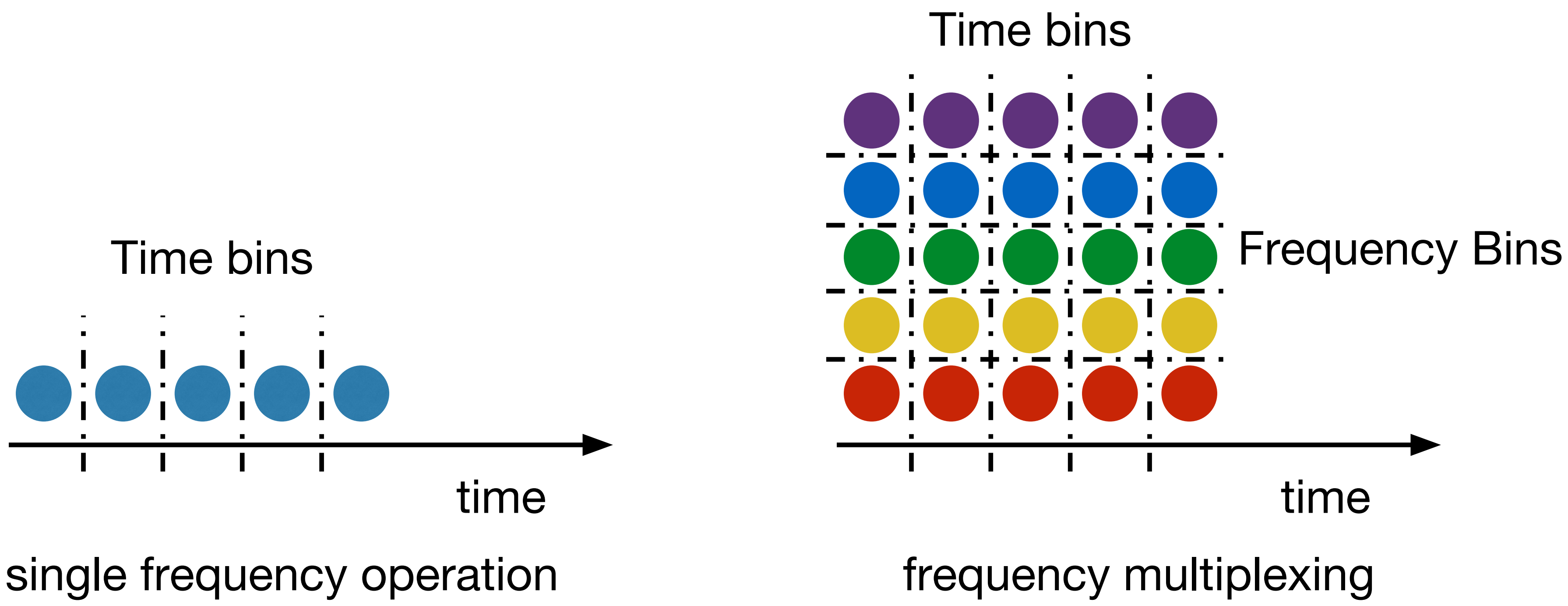
$$P(n{=}1) = \sum_{L} \sum_{n_A} \overbrace{P(n_A|\mathcal{I}_L)}^{\text{Generation Fidelity}} P(\mathcal{I}_L) \left[\sum_{N} \overbrace{P(n{=}1|\mathcal{S}_N, n_A)}^{\text{Release Fidelity}} P(\mathcal{S}_N|n_A) \right]$$



- *Numerical Example:*
- Q_L : $2{\cdot}10^7$
- Q_{iD} : $2{\cdot}10^4$
- On-off time : 60 ps
- Latency : 30 ps
- Detector efficiency : 99%
- Release fidelity : 99%
- Generation fidelity : 98%
- **Success Probability: 72%**

Currently on-going: use frequency multiplexing to reach > 99% overall efficiency

Frequency Multiplexing



- Modified protocol
  - In each time bin, pairs at multiple frequencies are generated
  - There are many low-Q idler outputs corresponding to different frequencies
  - Generation of one photon at any frequency in any of the time bins heralds a success
  - Efficient frequency conversion at the end of the clock cycle (Li et. al. CLEO 2015)

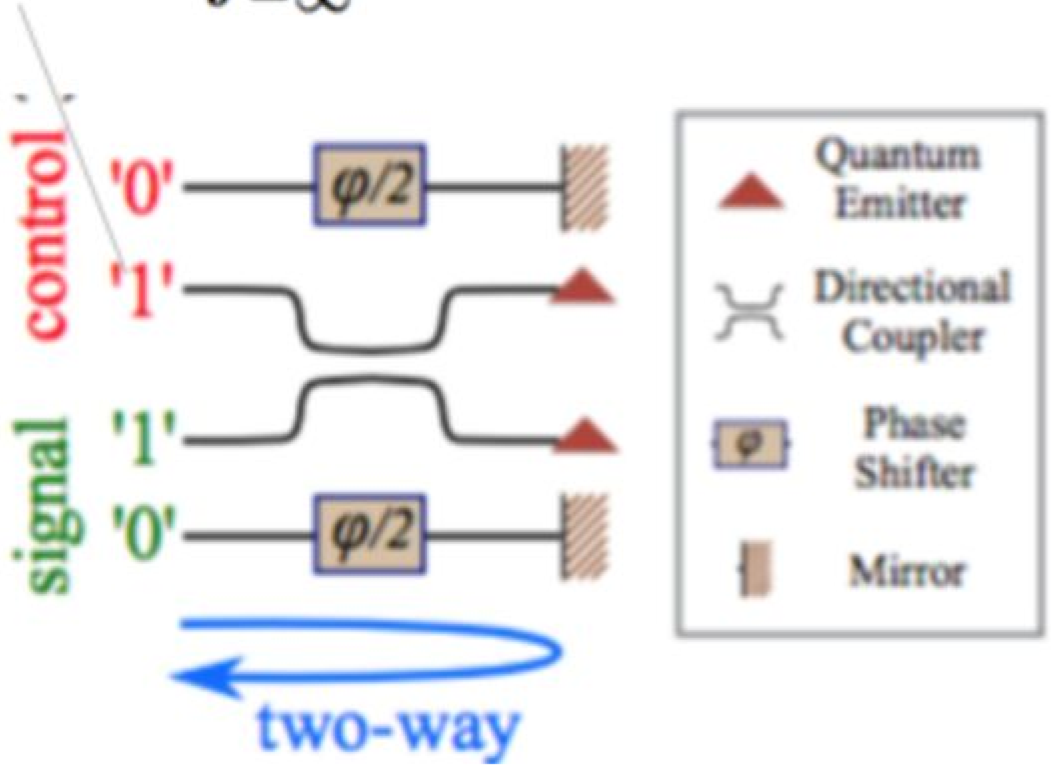
- Increases the number of attempts at pair generation by the number of frequencies

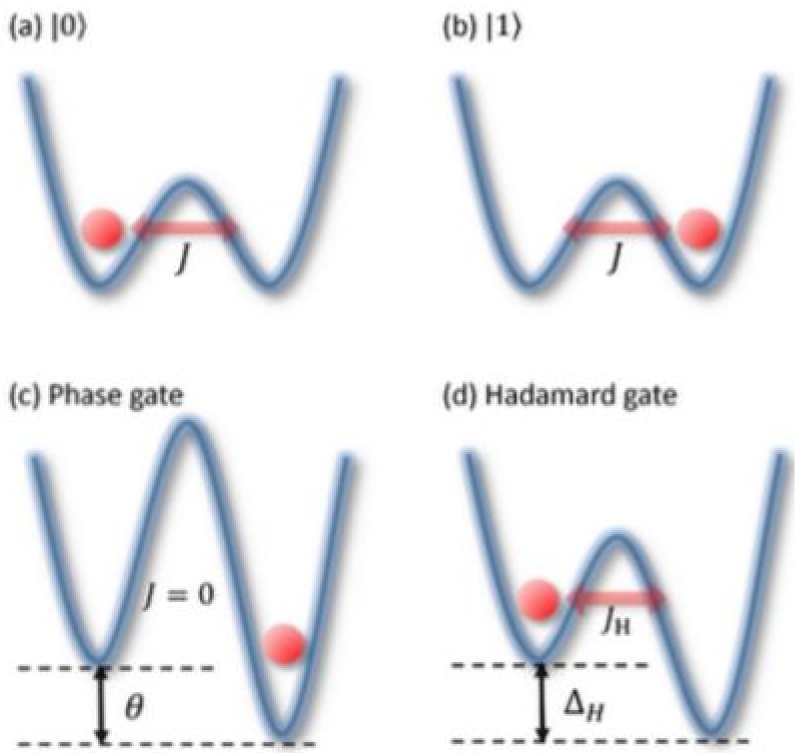
- **Success probability >90%** can be achieved by multiplexing over 5 frequencies with the same parameters used in the single frequency operation
- Success probability > 99% appears possible assuming detection efficiency >99.5%

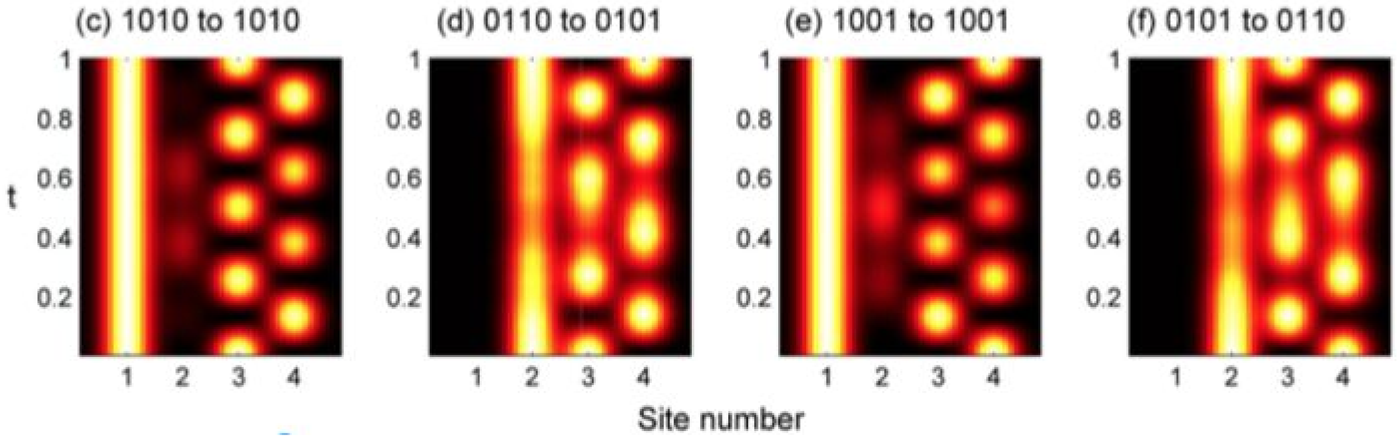
In-line nonlinearities?

- **Two-photon interactions with in-line nonlinearities**
  - Proposal for a passive two-photon controlled-phase gate using intrinsic nonlinearities of two-level emitters: manuscript to be submitted Sept 2016 [Lahini et al, ArXiv:1501.04349]
  - Quantum Logic with Interacting Bosons in 1D: manuscript under review [Nysteen, .. Englund]

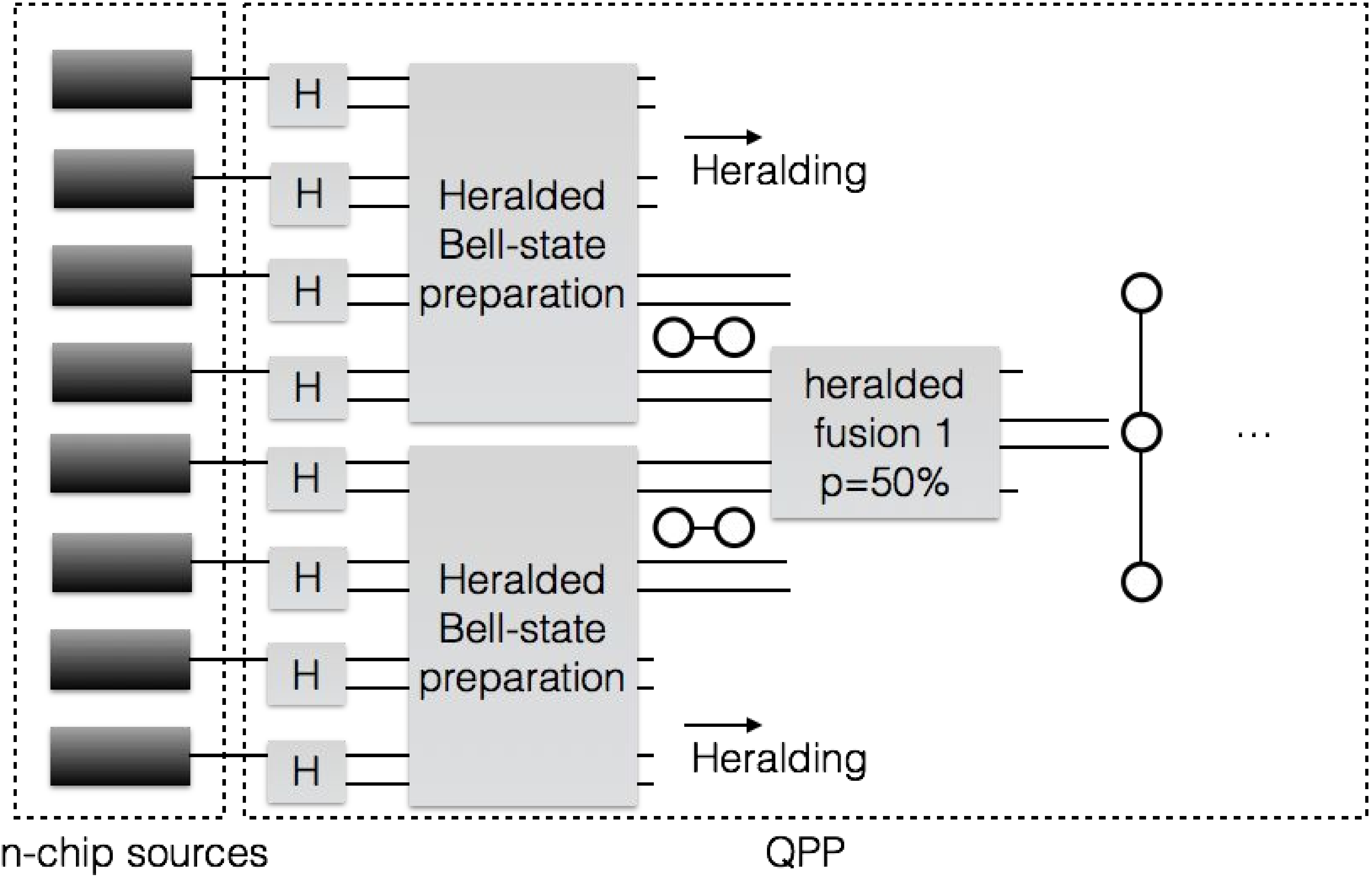
$$|\bar{1}_c\rangle = \int_{-\infty}^{\infty} \mathrm{d}k\, \xi(k) t(k)\, a^{\dagger}_{1c}(k)|\phi\rangle$$





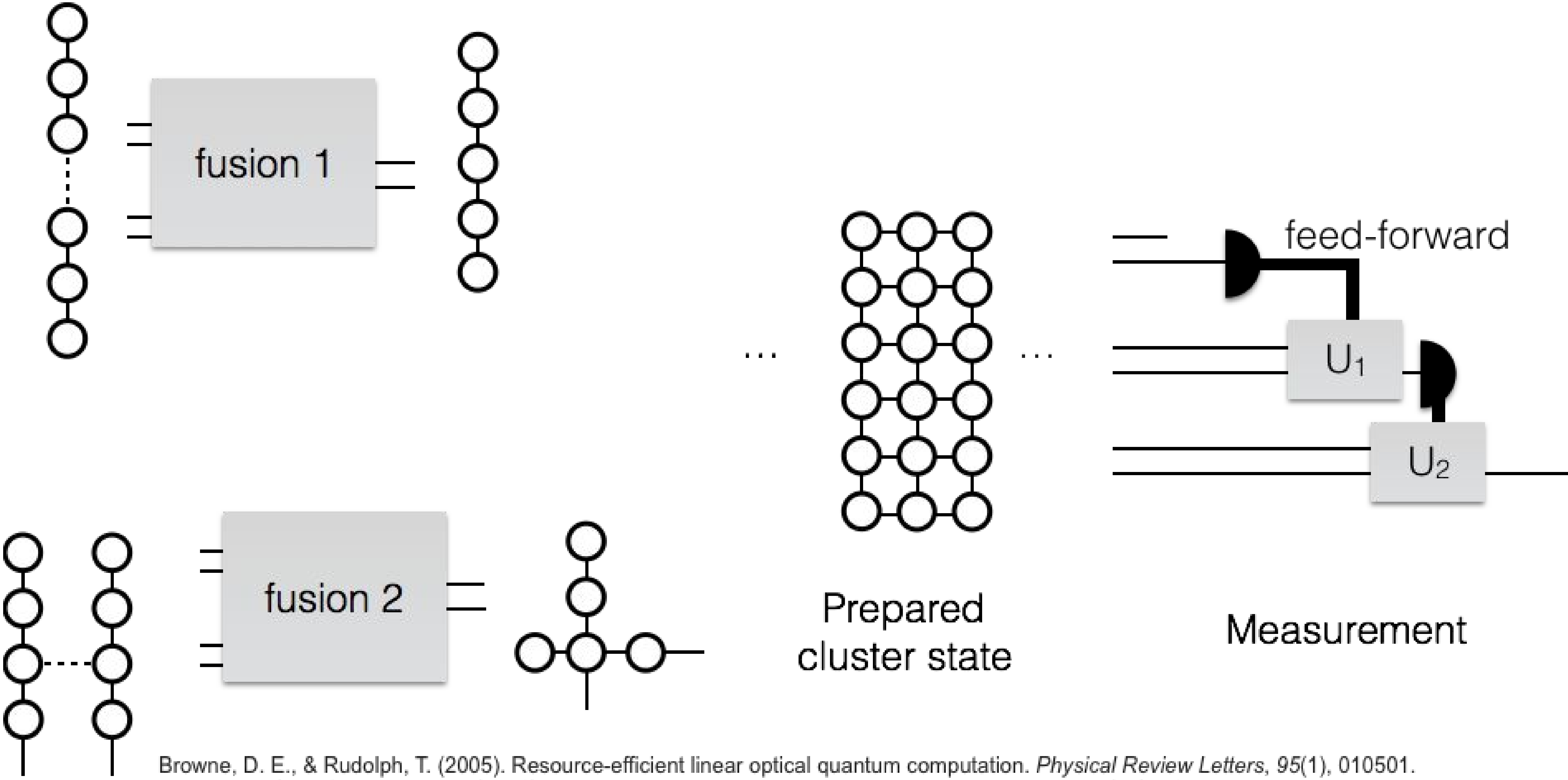


How to produce large cluster states on PICs?



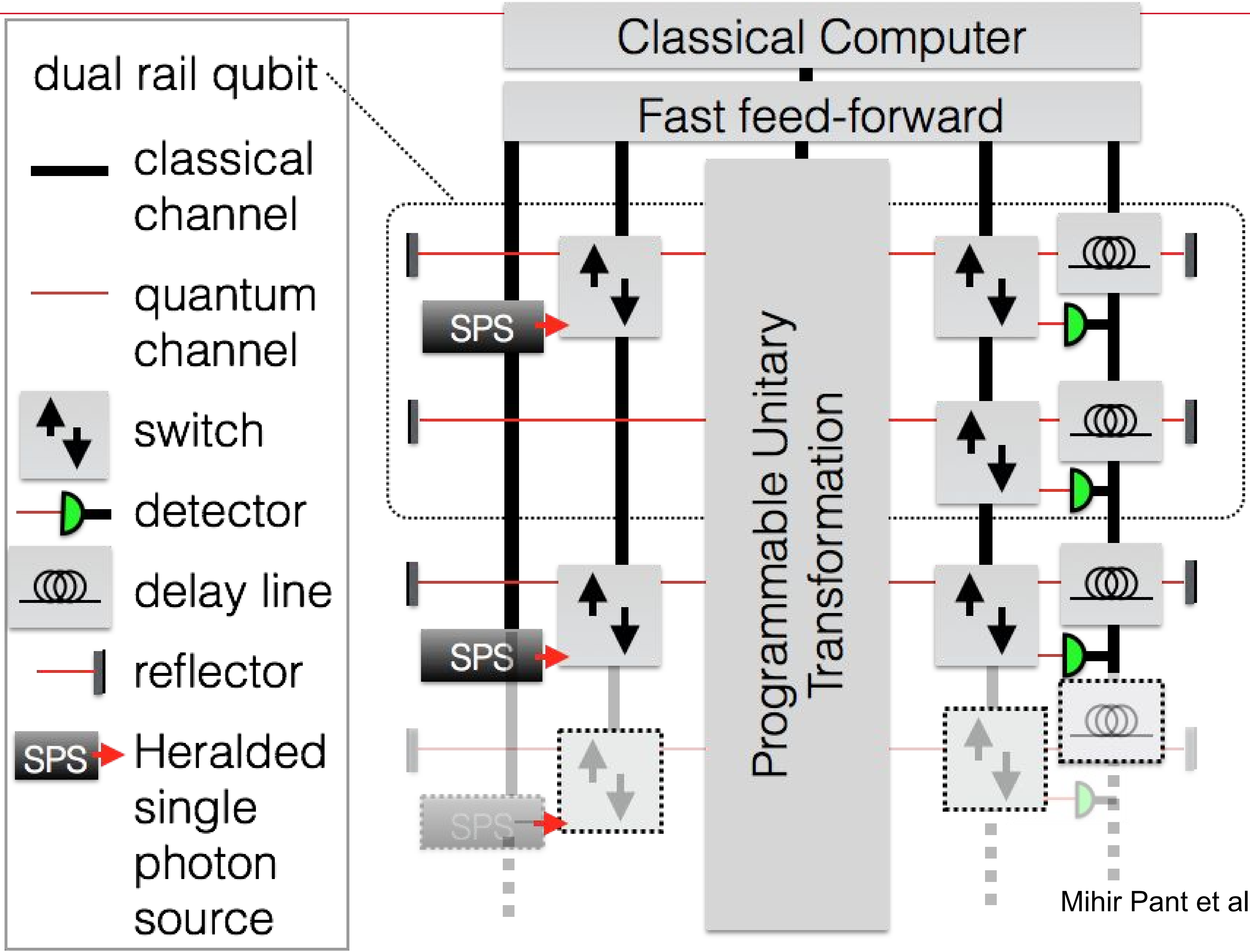
Browne, D. E., & Rudolph, T. (2005). Resource-efficient linear optical quantum computation. *Physical Review Letters*, *95*(1), 010501.
Zhang, Q., Bao, X. H., Lu, C. Y., Zhou, X. Q., Yang, T., Rudolph, T., & Pan, J. W. (2008). Demonstration of a scheme for the generation of "event-ready" entangled photon pairs from a single-photon source. *Physical Review A*, *77*(6), 062316.

Cluster state generation



Browne, D. E., & Rudolph, T. (2005). Resource-efficient linear optical quantum computation. *Physical Review Letters*, *95*(1), 010501.
Raussendorf, R., & Briegel, H. J. (2001). A one-way quantum computer. *Physical Review Letters*, *86*(22), 5188.

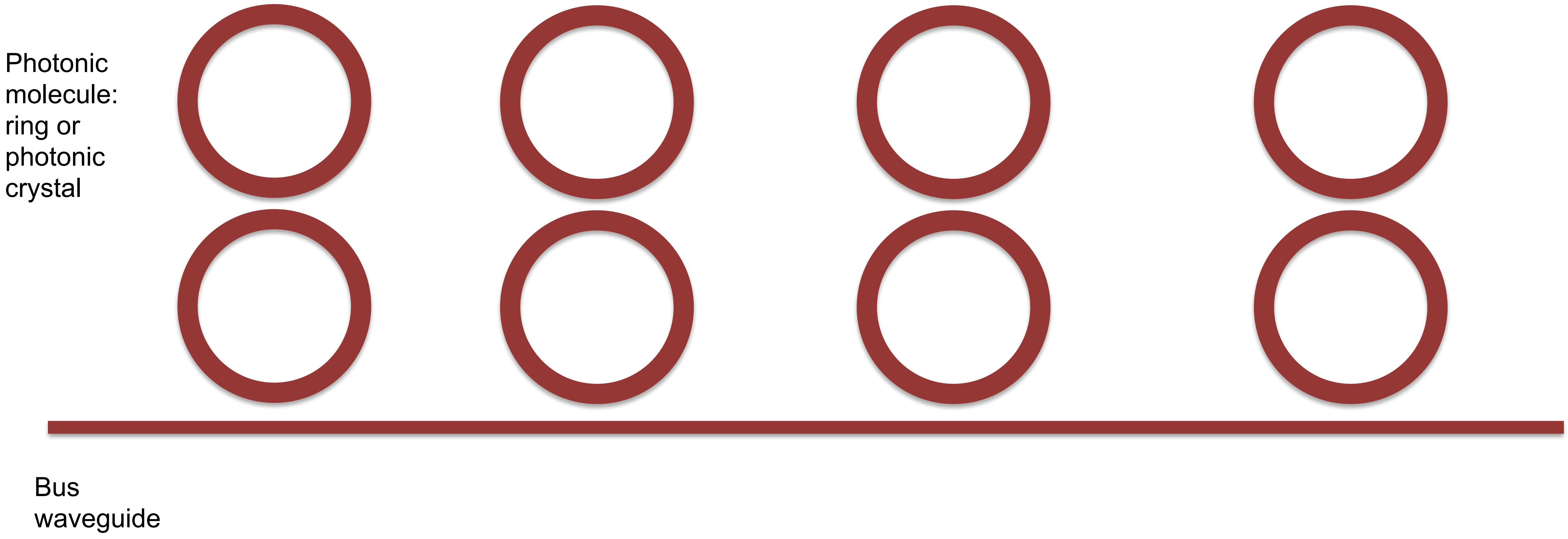
A Cluster State Architecture with photon storage



Mihir Pant et al

Nanophotonics Outlook

- **Challenges and future directions**
  - Devices for microcluster state generation : off-line nonlinearity resource
  - Strong coupling at room temperature : in-line nonlinearity resource
  - Scaling full-system architectures

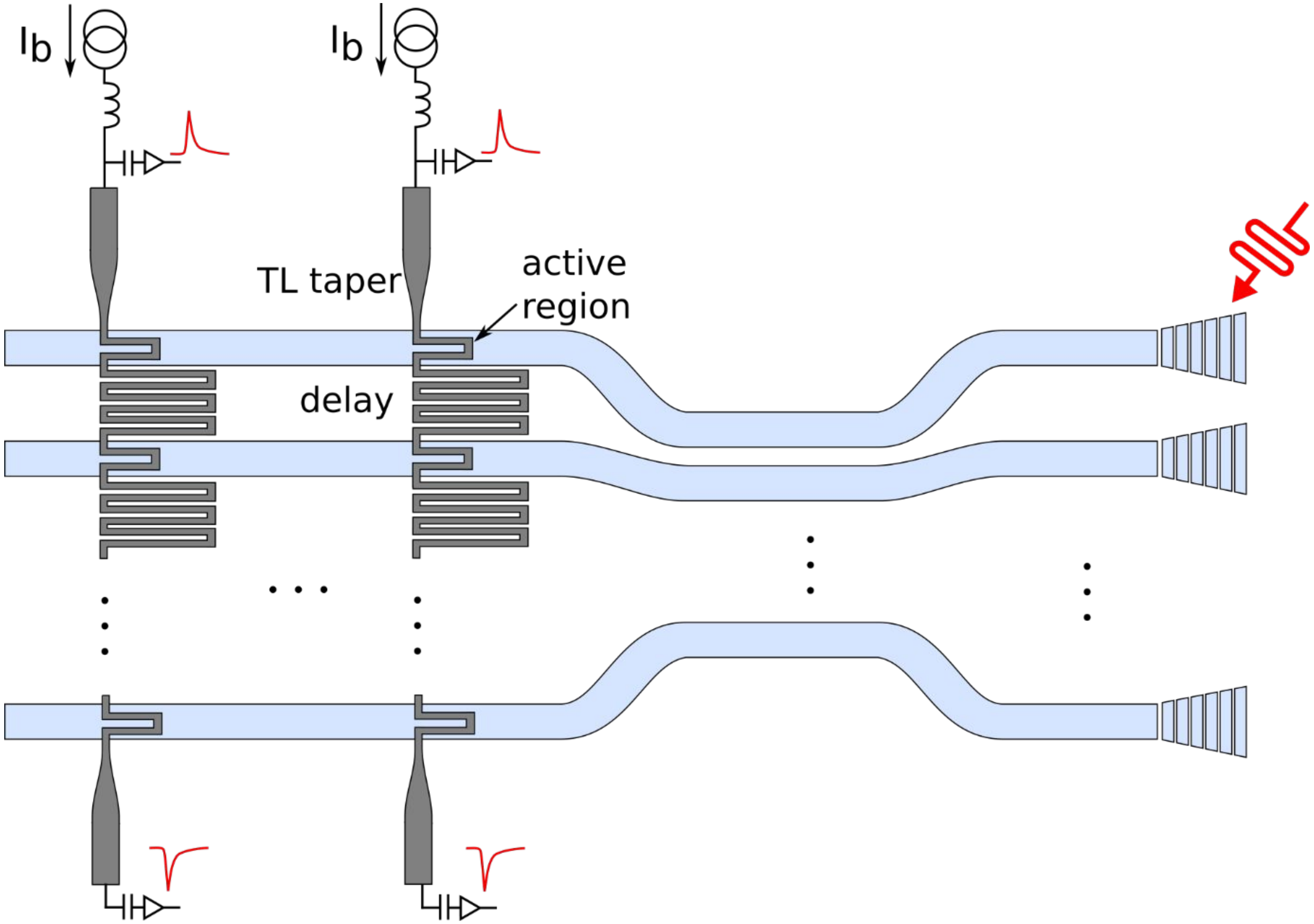


SEQUOIA nanophotonics summary

- **Programmable linear optics transformations**
  - Single-qubit gate infidelities < 10^{-7}
  - PIC demonstrated with up to 26 individually connected output modes
  - III-Nitride photonics platform
- **High-performance light sources**
  - Review of single photon sources: manuscript accepted for publication in Nature Photonics
  - On-Demand Single Photon emission based on quantum feedback control of a microcavity: manuscript to be submitted Sept 2016
  - 3-photon GHZ source based on 6-wave mixing
  - On-demand GHZ source based on QND and dynamic cavity control
- **Two-photon interactions with in-line nonlinearities**
  - Proposal for a passive two-photon controlled-phase gate using intrinsic non-linearities of two-level emitters: to be submitted Sept 2016
  - Quantum Logic with Interacting Bosons in 1D: in review
- **Challenges and future directions**
  - Devices for microcluster state generation : off-line nonlinearity resource
  - Strong coupling at room temperature : in-line nonlinearity resource
  - Programmable PICs
  - System-level picture of cluster state generator and general-purpose quantum computer using networked nonlinear qubit sys

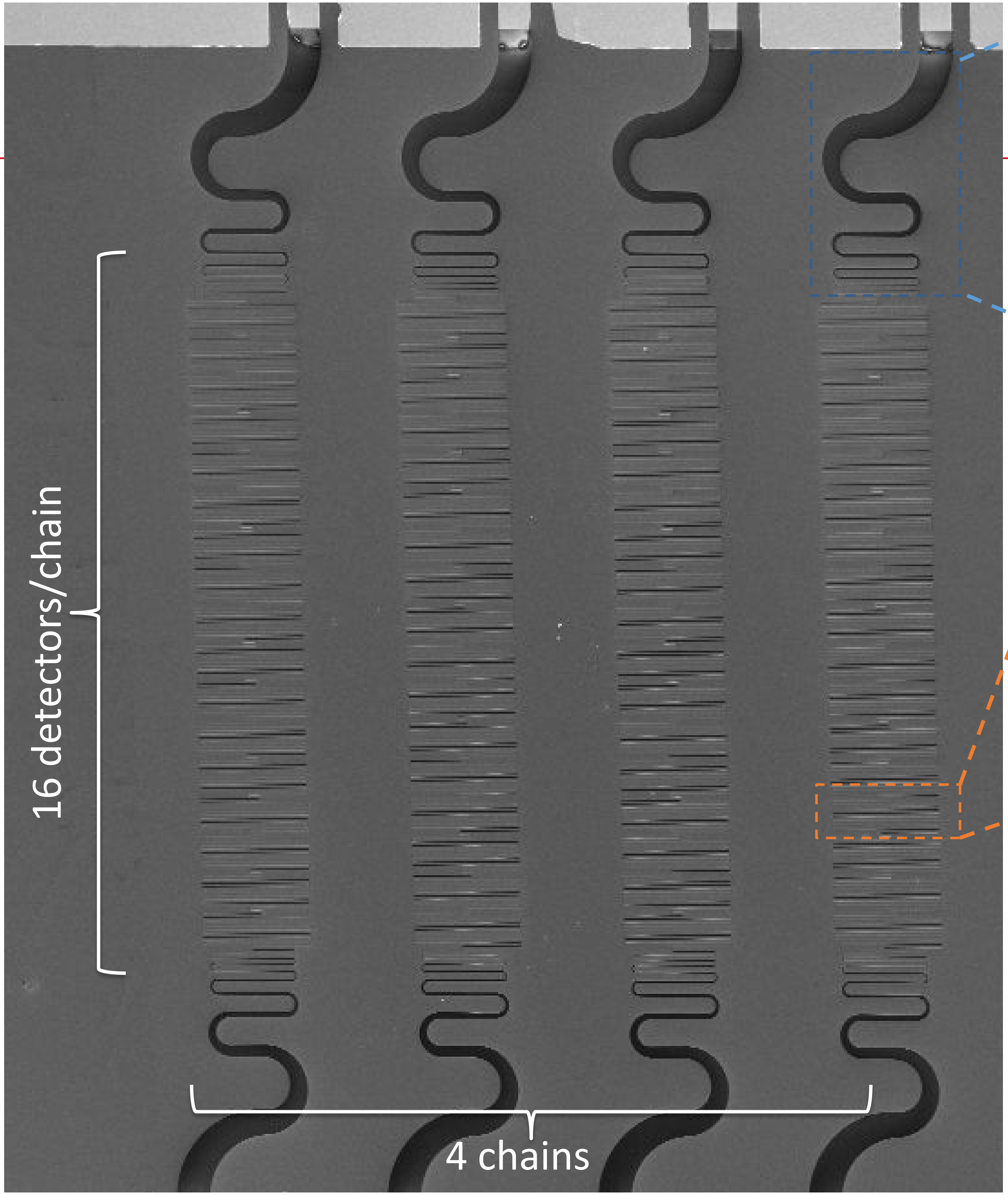
SEQUOIA detectors summary

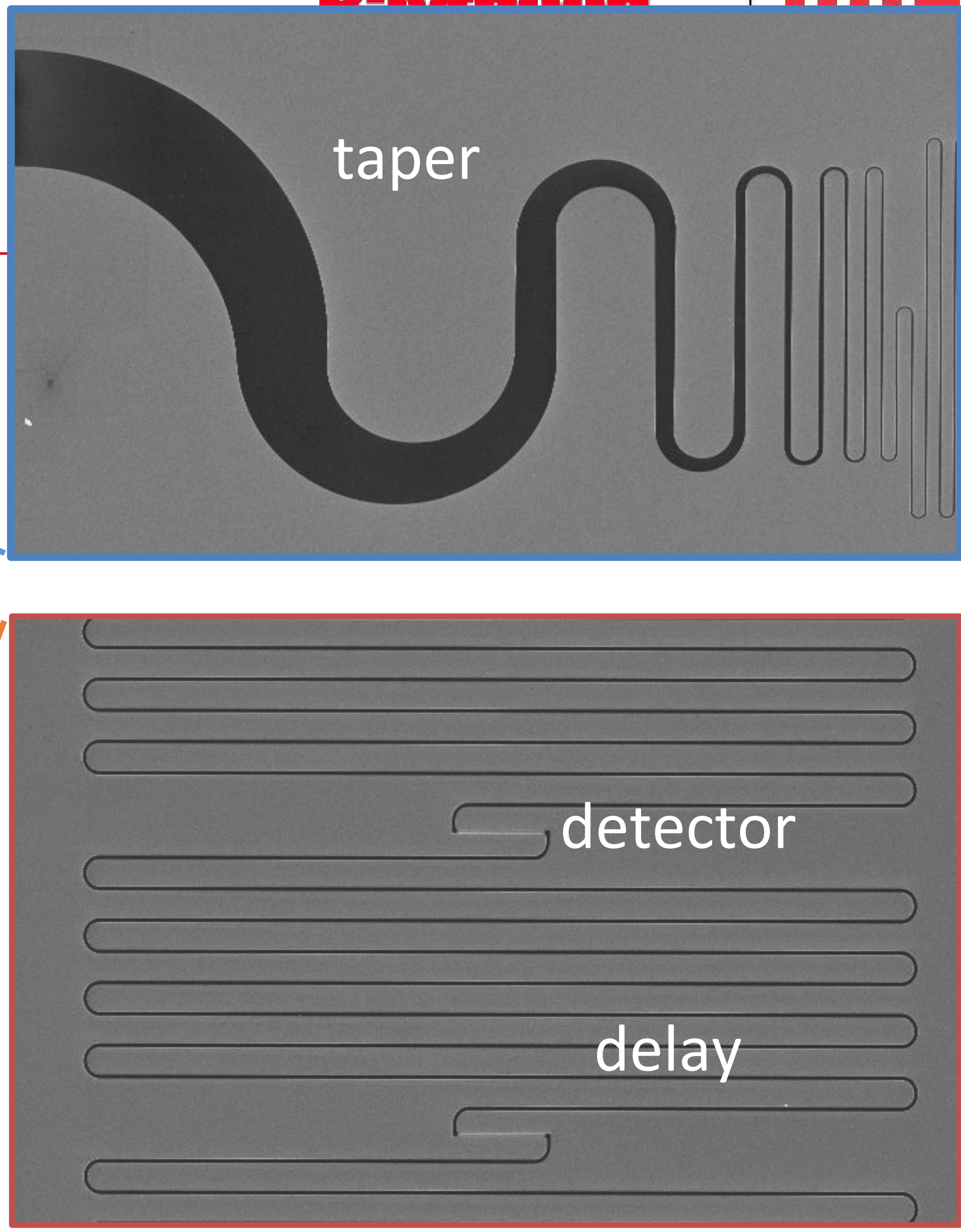
1. Developed method to read from 64 detectors simultaneously using differential readout
2. Proof-of-concept demonstration in AlN

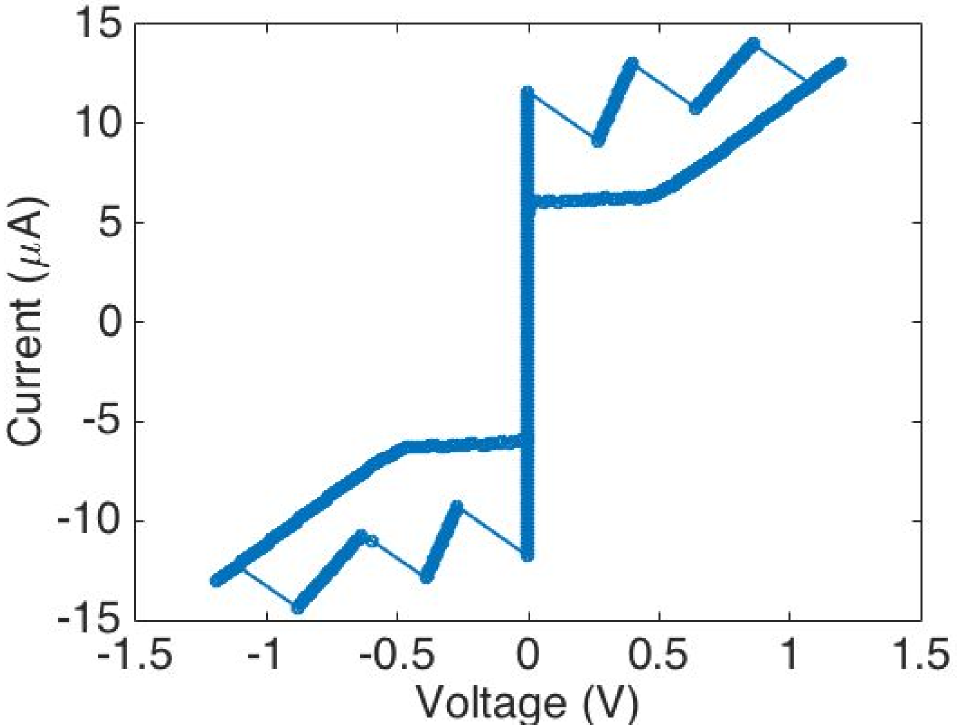


Impedance matched readout of 4 detector chains

Each chain consists of 16 detectors, all integrated on AlN waveguide

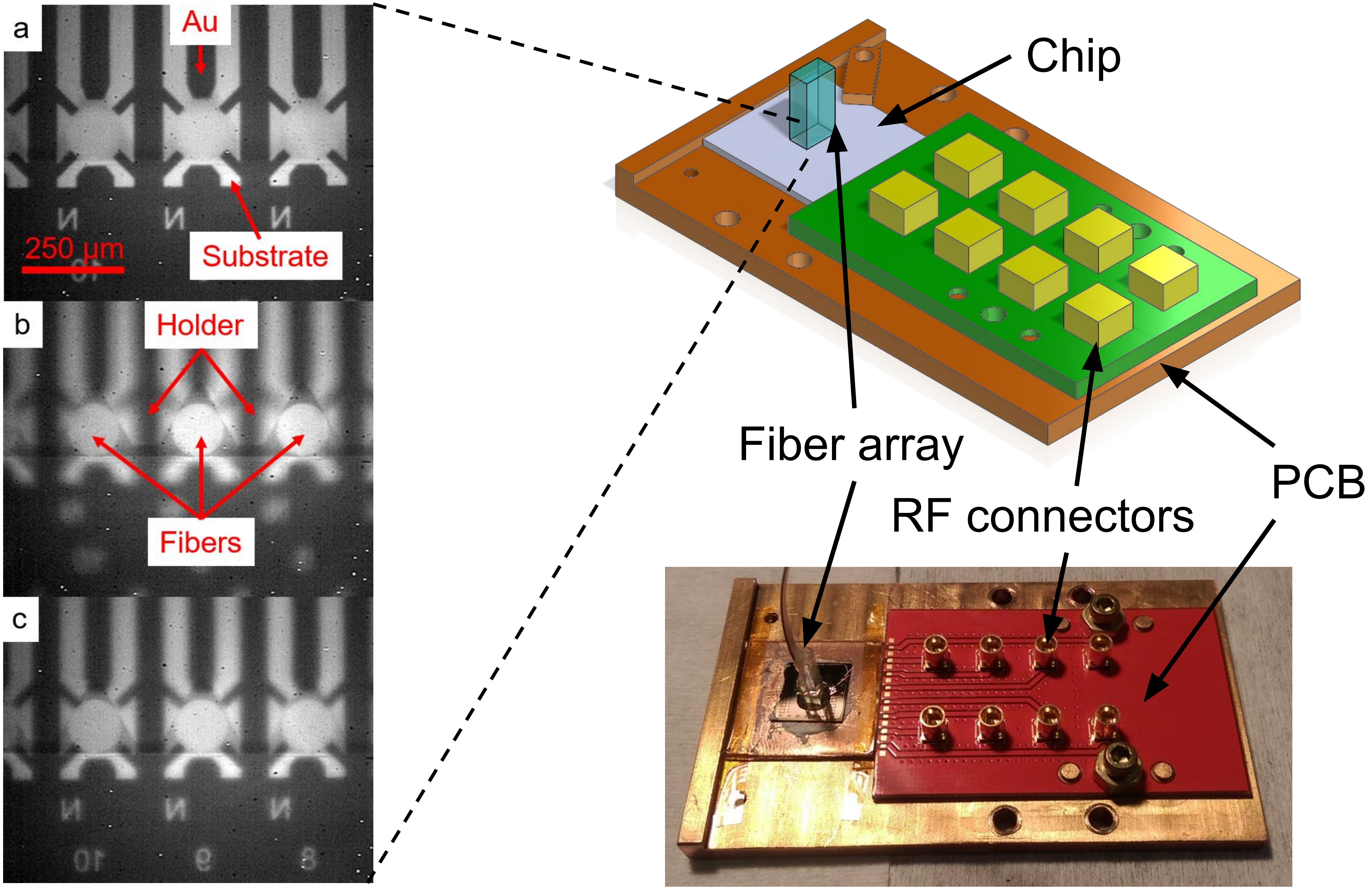

16 detectors/chain
4 chains


taper
detector
delay

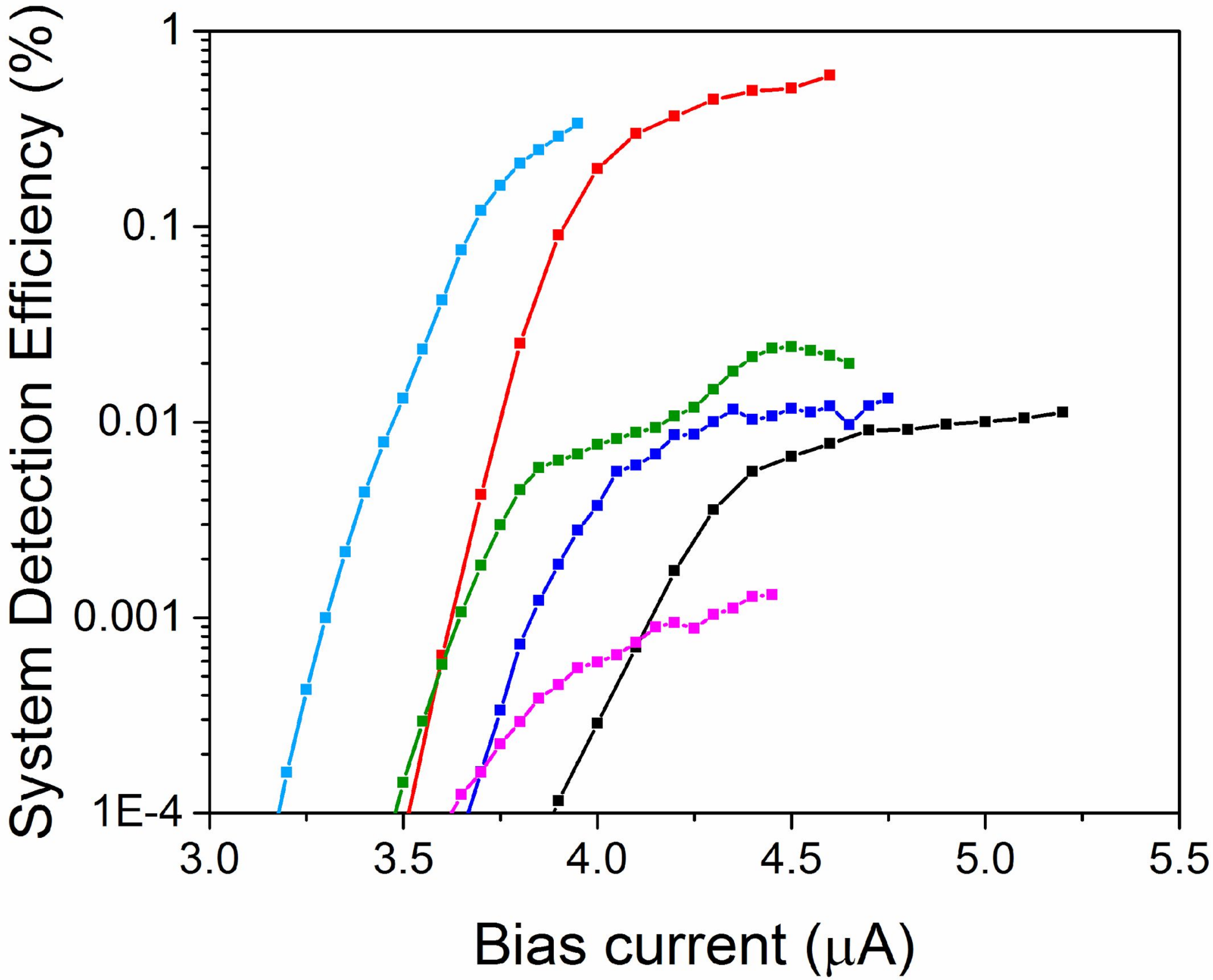

15
10
5
0
-5
-10
-15
Current (μA)
-1.5
-1
-0.5
0
0.5
1
1.5
Voltage (V)

Detectors summary

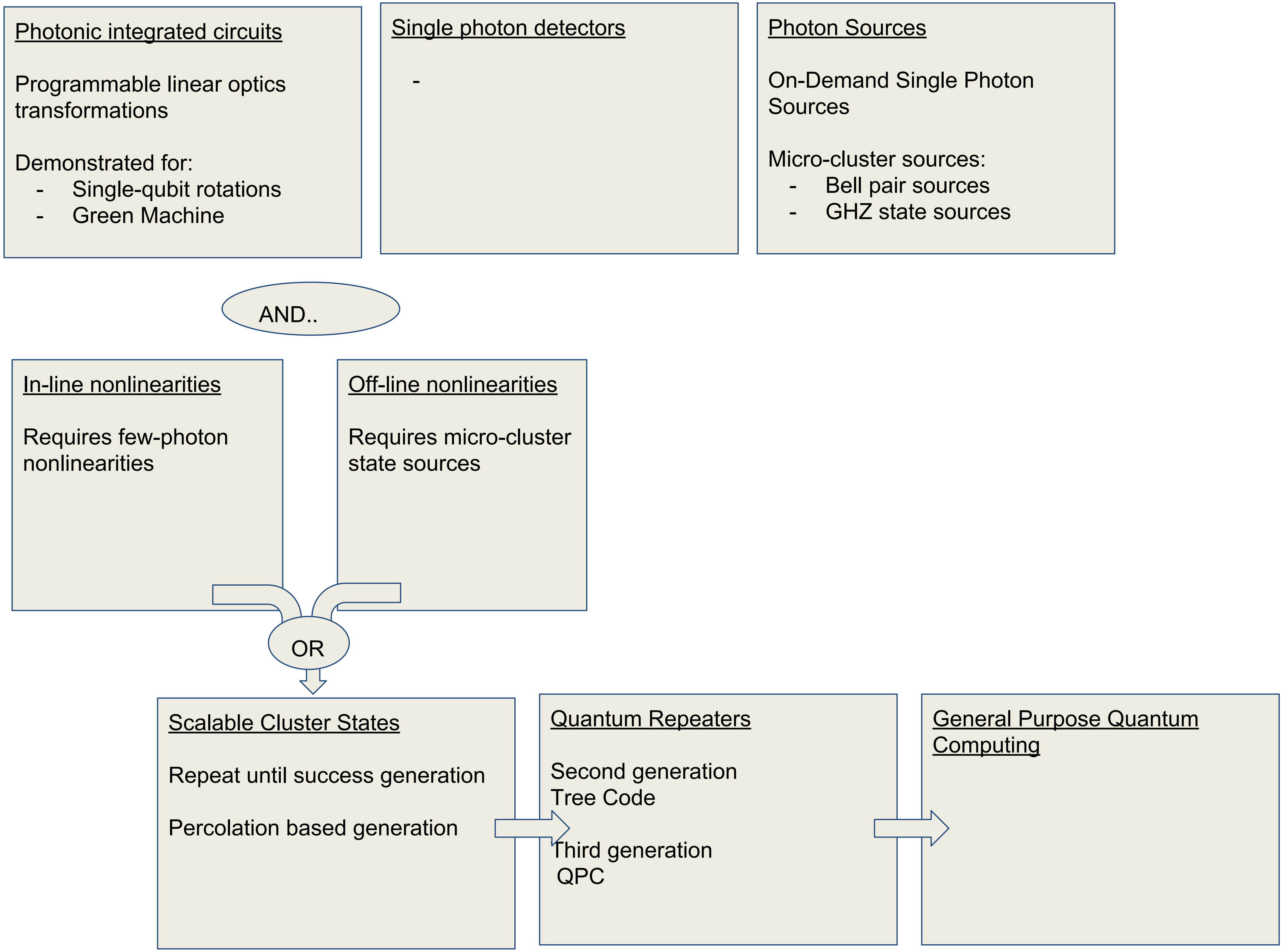
Developed compact SNSPD packaging and readout



System detection efficiency and reset time of eight SNSPDs



Overview



Photonic integrated circuits

Programmable linear optics transformations

Demonstrated for:

- Single-qubit rotations
- Green Machine

Single photon detectors

-

Photon Sources

On-Demand Single Photon Sources

Micro-cluster sources:

- Bell pair sources
- GHZ state sources

AND..

In-line nonlinearities

Requires few-photon nonlinearities

Off-line nonlinearities

Requires micro-cluster state sources

OR

Scalable Cluster States

Repeat until success generation

Percolation based generation

Quantum Repeaters

Second generation
Tree Code

Third generation
QPC

General Purpose Quantum Computing

LOQC Program Vision

- Theory and protocols
  - Novel ECC methods: graph codes, finite-length percolation, ECC for mode mismatch and excess noise
  - Hybrid qubit modes: CV clusters for universal QC with PNR
  - Special-purpose QC: annealing, repeaters, quantum nodes
  - Novel ways to incorporate weak non-linearities for universal QC
- Nano-photonics
  - High-rate high-quality sources of 3-qubit (or larger) microclusters
  - Exploiting non-linear quantum optics in novels ways (e.g., high-order NL, complex photonic molecule structures) for qubit encoding and interactions
  - On-chip detectors & feed-forward
- Single photon detectors
  - Demonstration of scalable readout using time tagging
  - Electro-optic feed-forward
  - New room-temperature detector concepts: semiconductor absorber and Yamomoto-Haus QND approach
- Possible program goal
  - 5 yr: Demo of 3-qubit GHZ state generation with 99.99% Fidelity at 100 MHz
  - 5 yr: Translating SC circuit QED to optical: >> higher density, RT, networks
  - 5 yr: 10-qubit cluster produced with off-line nonlinearities
  - 10 yr: Demo 1 logical qubit (1 Rausendorf lattice block) w/ Ballistic QC, F = 99%
  - 15 yr: One all-optical quantum repeater that beats repeaterless performance

Back up slides (details)

Theory: detailed slides

General purpose LOQC

OVERVIEW OF LINEAR OPTICS QUANTUM COMPUTING

1. KLM 2001 SCHEME: SPS, FF, dynamic-reconfigurable PNP
   - Original scheme: Feedforward; entangled ancilla clusters for efficient operation
   - Improved schemes: Boosted fusion gates
2. BALLISTIC CLUSTER STATE: SPS, FF only at state prep and cluster measurement
   - Sources of entangled 3-5 photon cluster fragments improve resource requirements
   - Small multi-photon entangled measurements help

3. Quantum computing using stored photons

   - No nonlinearities: scalable architecture for LOQC and cluster state quantum computing (Ballistic or non-ballistic)
   - With parametric nonlinearities (Kerr, chi-2, atomic, etc)
     - Ising model
     - Parallels to superconducting quantum computing
       - Why is optics better than SCQC? Room temperature, 10^4 higher density; interfacing with telecom quantum networks/qubit distribution

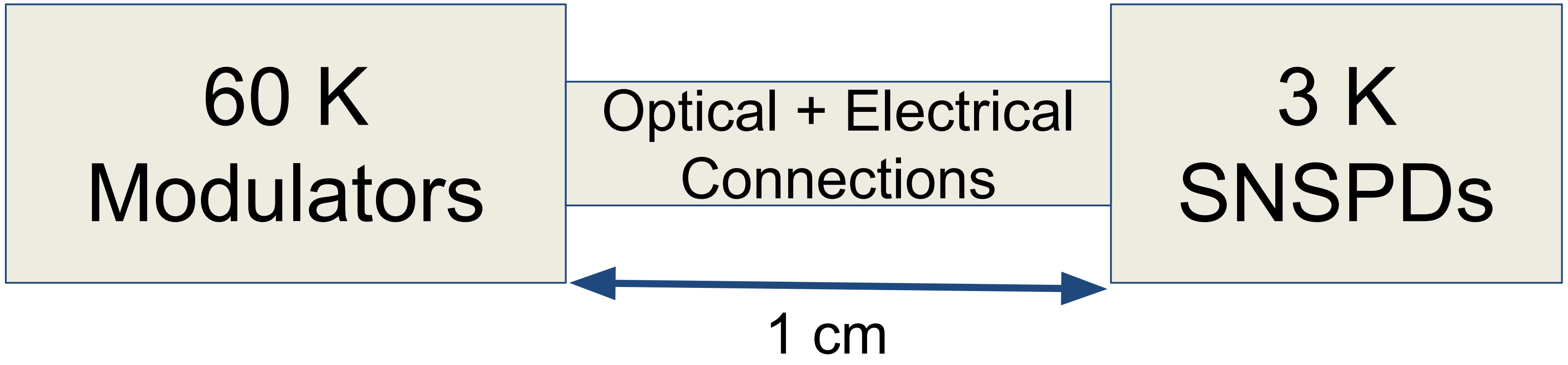
4. DV quantum computing using CV cluster

   Embed circuit model quantum computing into CV-cluster states by Olivier

   Use homodyne and direct detection

Nanophotonics: detailed slides

Design for SNSPD-integrated PICs



How powerful does the cryostat need to be?

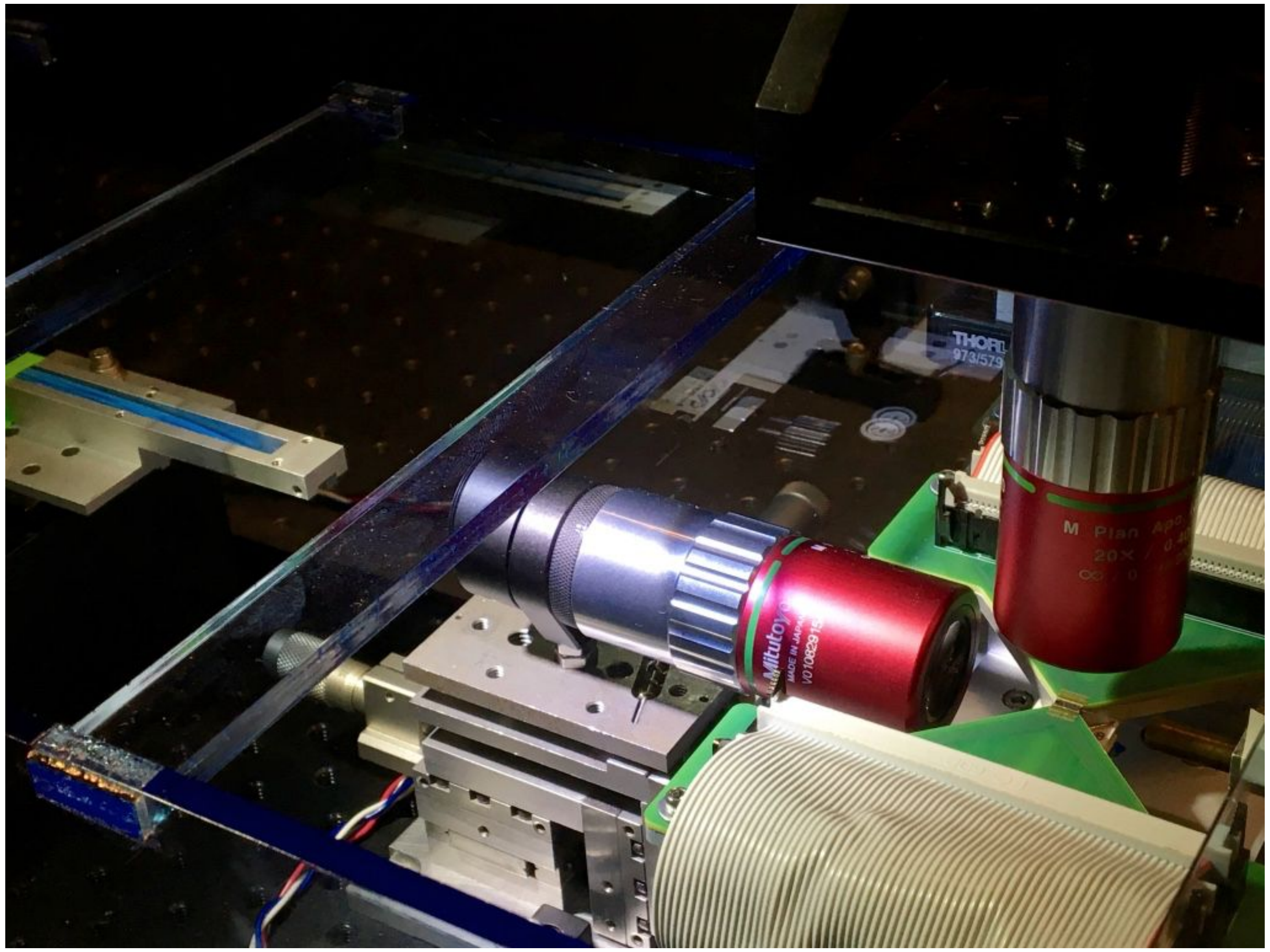
Optical connections: 220 nm X 500 nm silicon waveguides surrounded by 10um X 10 um X 10 um silica: **1.7 uW/waveguide**

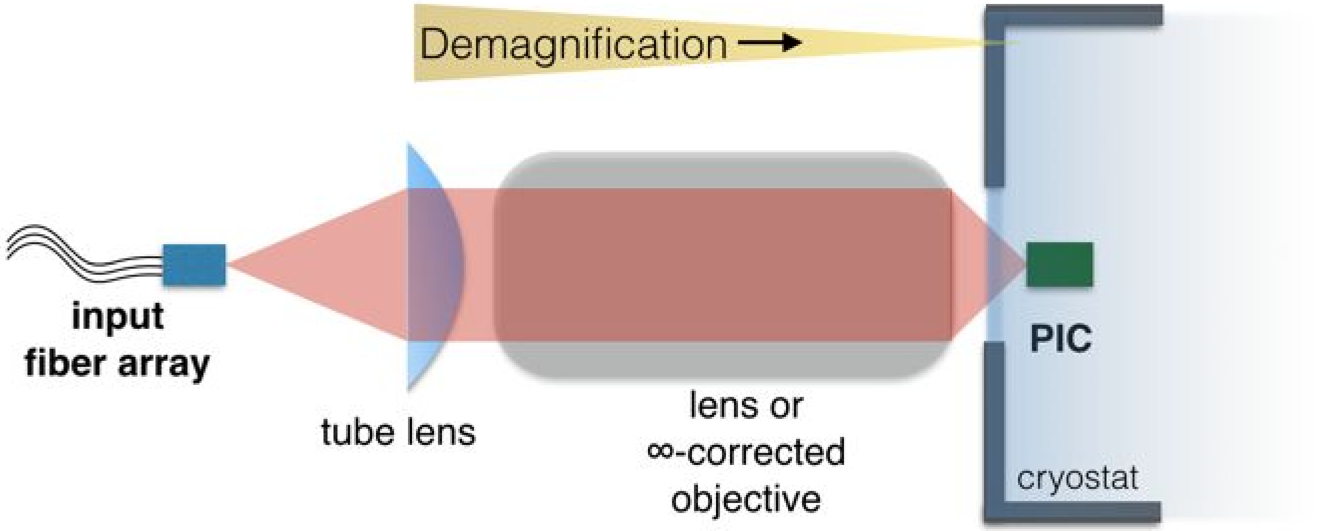
Electrical connections: 15 um diameter gold : **1.3 mW/wire**

Radiation: **18uW** assuming 5mm X 5mm radiative surface

Takeaway: the major contribution comes from electrical connections.

Design for SNSPD-integrated PICs





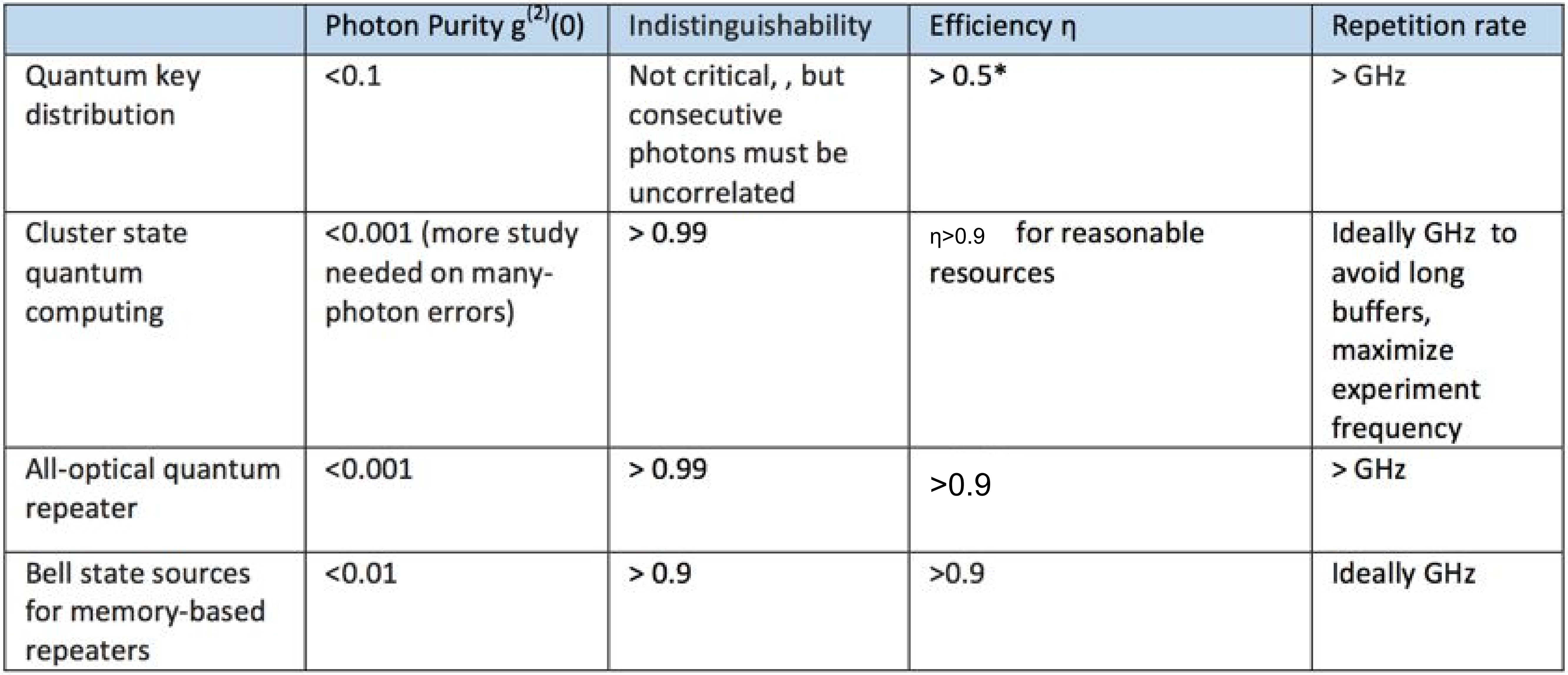
- PNP1b: ~8.5dB measured coupling loss per free-space-coupled facet
- Losses predominantly due to aperture clipping in objectives and surface irregularity in lenses

Low-temp, high-speed PICs concept

Design for electro-optic version of PNP using rings

NEMS approach

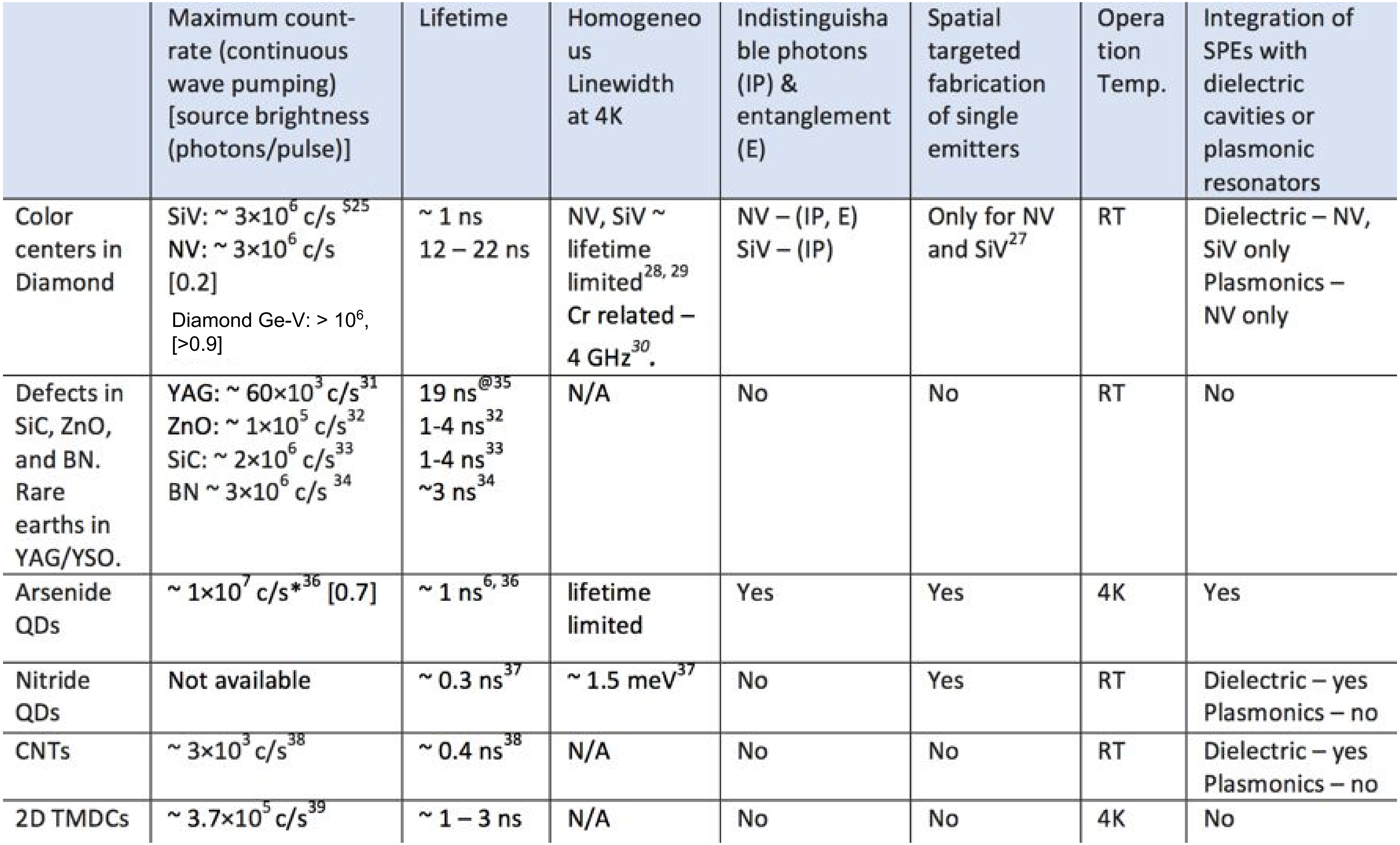
How good of a single photon source needed?



	Photon Purity $g^{(2)}(0)$	Indistinguishability	Efficiency η	Repetition rate
Quantum key distribution	<0.1	Not critical, , but consecutive photons must be uncorrelated	> 0.5*	> GHz
Cluster state quantum computing	<0.001 (more study needed on many-photon errors)	> 0.99	η>0.9 for reasonable resources	Ideally GHz to avoid long buffers, maximize experiment frequency
All-optical quantum repeater	<0.001	> 0.99	>0.9	> GHz
Bell state sources for memory-based repeaters	<0.01	> 0.9	>0.9	Ideally GHz

** - to be competitive against attenuated laser QKD with decoy state*

Atom-like single photon sources



	Maximum count-rate (continuous wave pumping) [source brightness (photons/pulse)]	Lifetime	Homogeneous Linewidth at 4K	Indistinguishable photons (IP) & entanglement (E)	Spatial targeted fabrication of single emitters	Operation Temp.	Integration of SPEs with dielectric cavities or plasmonic resonators
Color centers in Diamond	SiV: ~ 3×10^{6} c/s [\$25] NV: ~ 3×10^{6} c/s [0.2] Diamond Ge-V: > 10^{6}, [>0.9]	~ 1 ns 12 – 22 ns	NV, SiV ~ lifetime limited[28, 29] Cr related – 4 GHz[30].	NV – (IP, E) SiV – (IP)	Only for NV and SiV[27]	RT	Dielectric – NV, SiV only Plasmonics – NV only
Defects in SiC, ZnO, and BN. Rare earths in YAG/YSO.	YAG: ~ 60×10^{3} c/s[31] ZnO: ~ 1×10^{5} c/s[32] SiC: ~ 2×10^{6} c/s[33] BN ~ 3×10^{6} c/s [34]	19 ns[@35] 1-4 ns[32] 1-4 ns[33] ~3 ns[34]	N/A	No	No	RT	No
Arsenide QDs	~ 1×10^{7} c/s*[36] [0.7]	~ 1 ns[6, 36]	lifetime limited	Yes	Yes	4K	Yes
Nitride QDs	Not available	~ 0.3 ns[37]	~ 1.5 meV[37]	No	Yes	RT	Dielectric – yes Plasmonics – no
CNTs	~ 3×10^{3} c/s[38]	~ 0.4 ns[38]	N/A	No	No	RT	Dielectric – yes Plasmonics – no
2D TMDCs	~ 3.7×10^{5} c/s[39]	~ 1 – 3 ns	N/A	No	No	4K	No

*Summary of photophysical properties of solid state SPEs. c/s – counts per second; N/A – not available. The reported count rates for each system can be potentially optimized by integrating with cavities, or improving collection optics. * - count rate at the objective, that is directly comparable to other systems. A brighter count rate of ~ 1×10^{7} c/s was reported for photons arriving at the first collection lens. @ - realized by optical upconversion to a short-lived excited state. \$ - reported from a nanodiamond on iridium. # - recorded from a nanodiamond positioned onto a solid immersion lens. In both cases emitters in bulk diamond are dimmer.*

Single photon sources as required for LOQC?

$P(n=1)>0.9$

$g^{(2)}(0)<0.01$ (more theory needed)

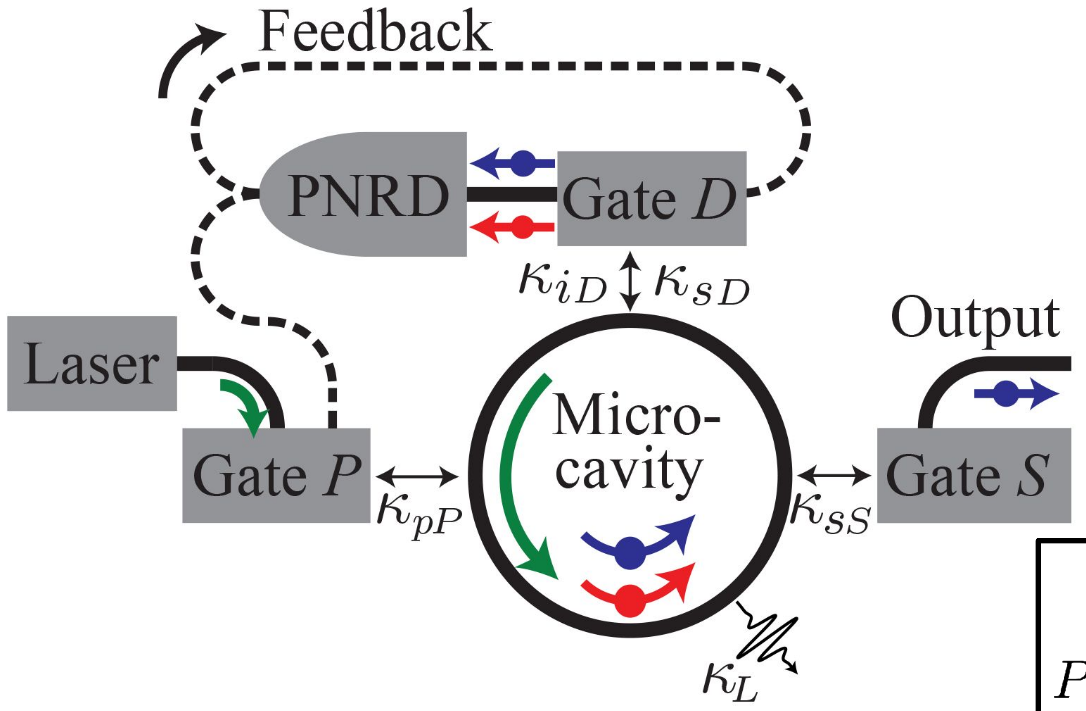
HOM visibility > 0.99

Suppose we use spontaneous pair generation. No published scheme reaches this performance. Mikkel Heuck, Mihir Pant, and DE proposed a new scheme that could work with reasonable technology.

Mikkel

Mihir

How to build a sufficient source?



Protocol

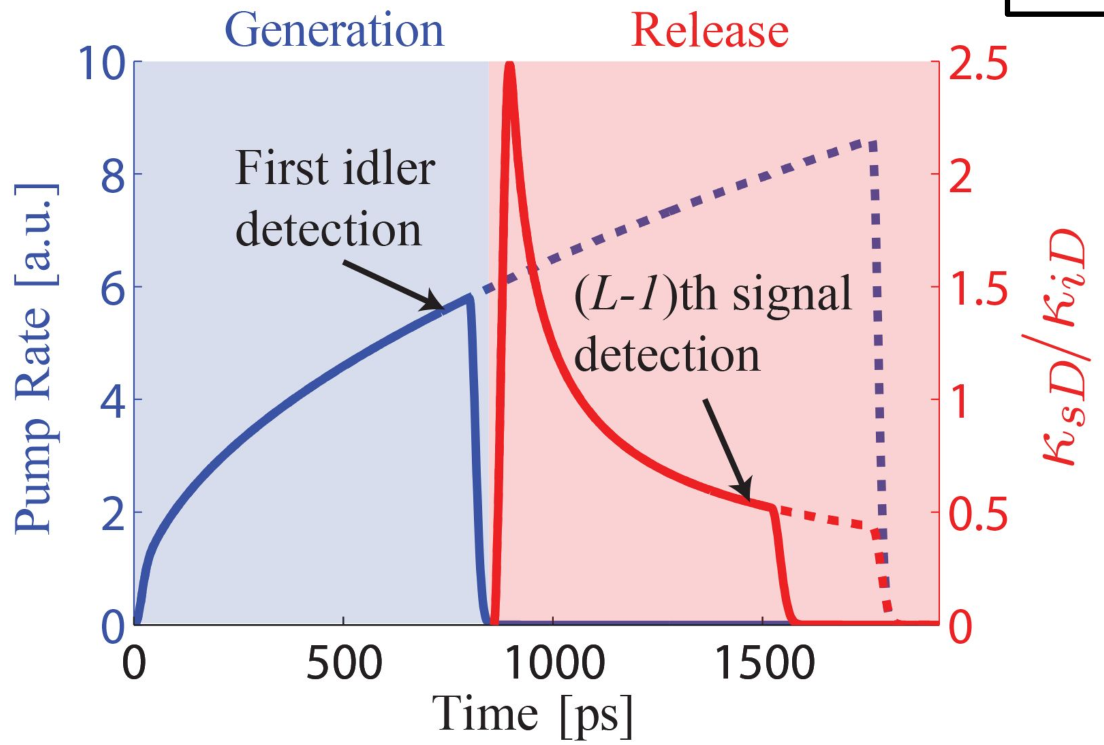
Generation

- Pump laser is turned off at the first idler detection.
- A total of n_A pairs are created and L idler photons are detected.

Release

- Coupling, κ_{sD}, is turned off at the (L-1)th signal detection.
- A total of N signal photons are detected.

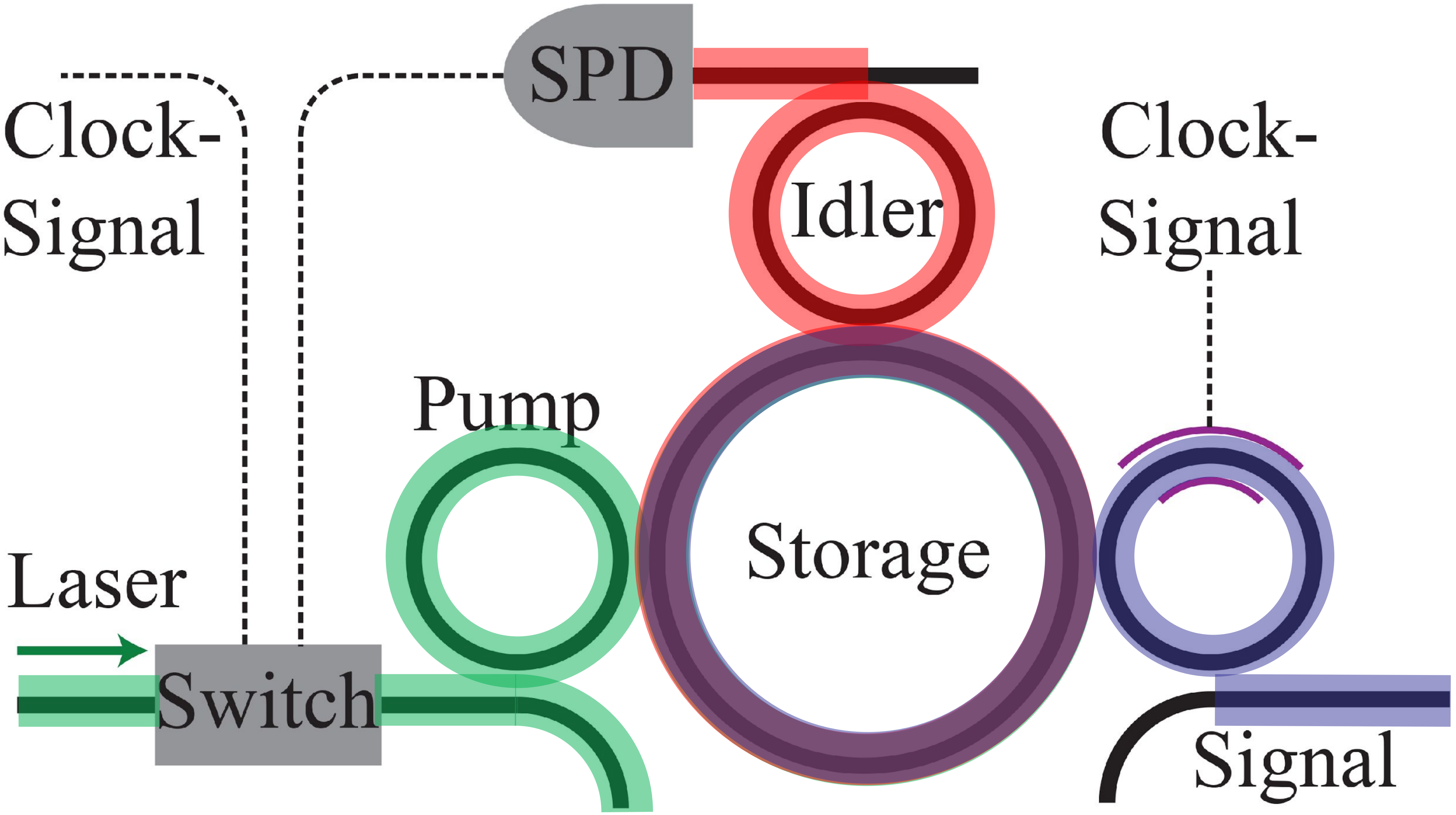
$$P(n=1) = \sum_{L} \sum_{n_A} \overbrace{P(n_A|\mathcal{I}_L)}^{\text{Generation Fidelity}} P(\mathcal{I}_L) \left[\sum_{N} \overbrace{P(n=1|\mathcal{S}_N, n_A)}^{\text{Release Fidelity}} P(\mathcal{S}_N|n_A) \right]$$



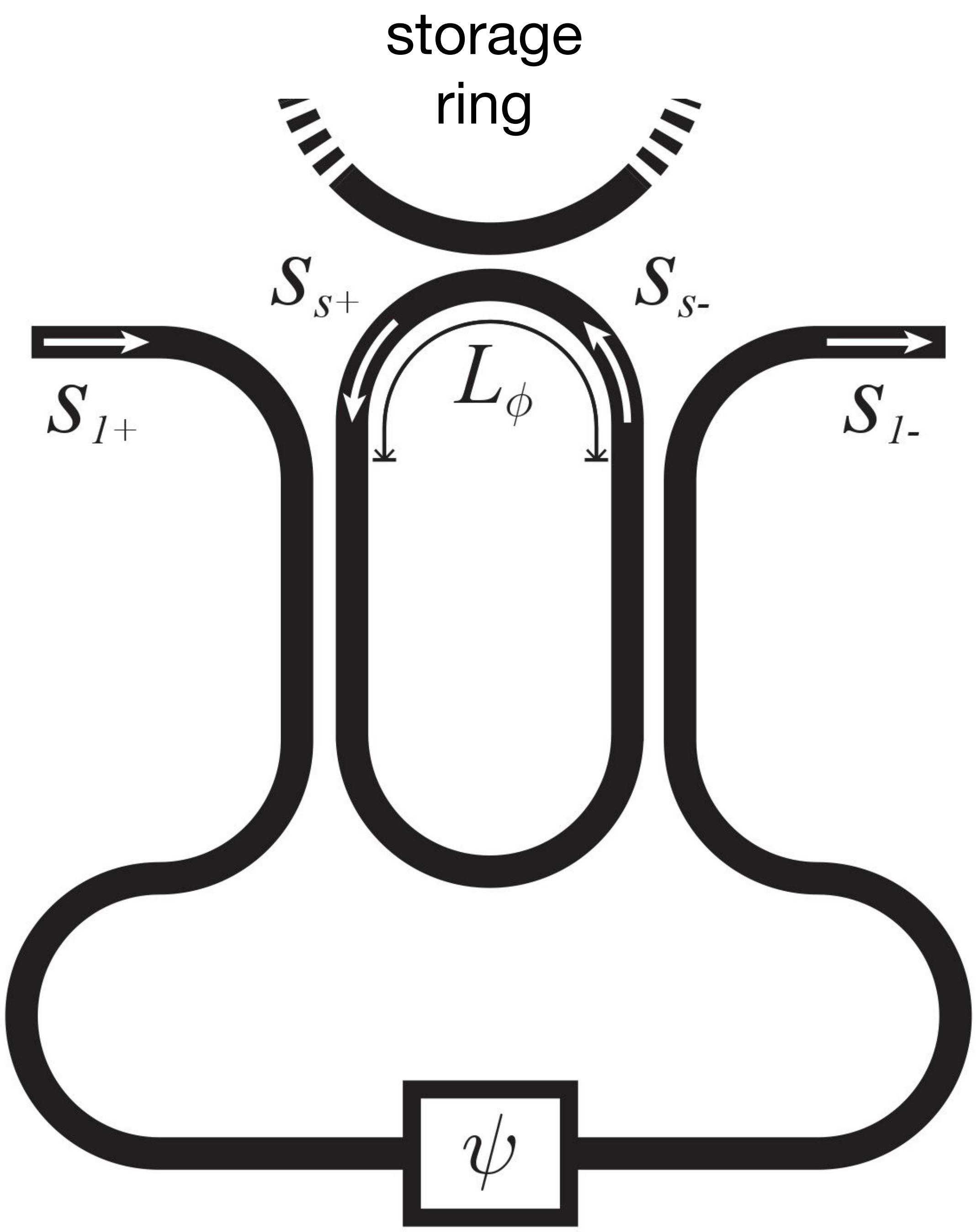
- *Numerical Example:*
- Q_L : $2{\cdot}10^7$
- Q_{iD} : $2{\cdot}10^4$
- On-off time : 60 ps
- Latency : 30 ps
- Detector efficiency : 99%
- Release fidelity : 99%
- Generation fidelity : 98%
- **Success Probability: 72%**

Currently on-going: use frequency multiplexing to reach > 99% overall efficiency

The Device Structure - Protocol

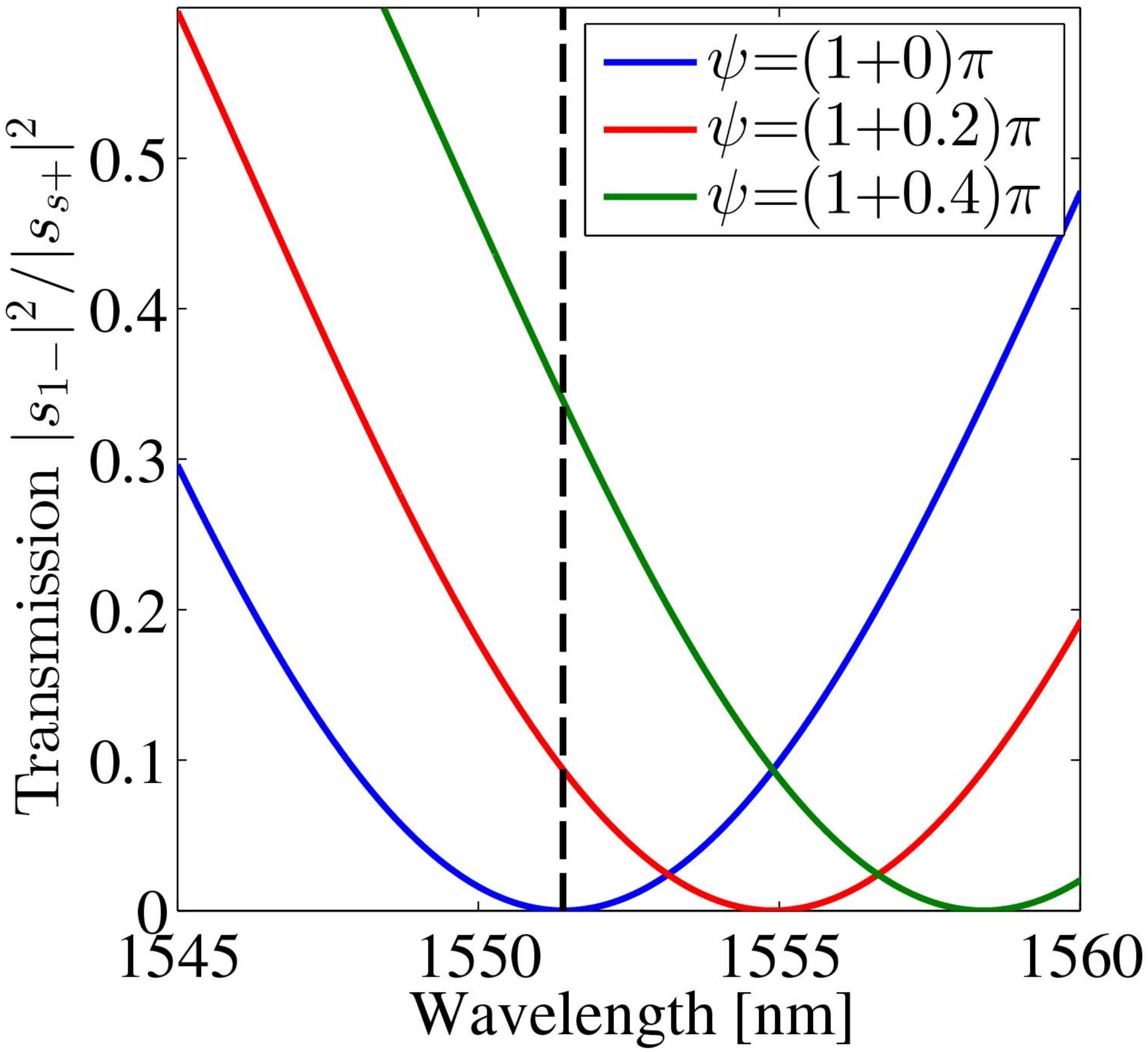


The Device Structure – Gate Structure

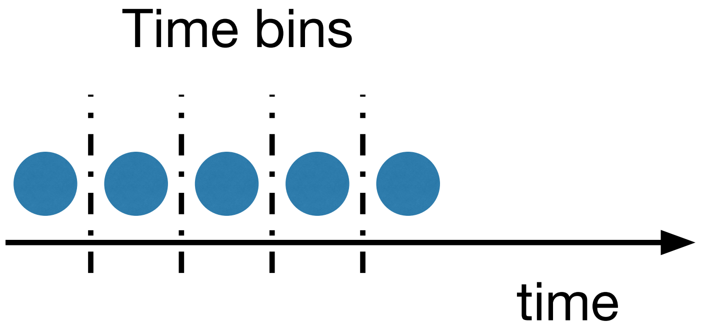


Darmawan *et al*. Optics Express (2007)

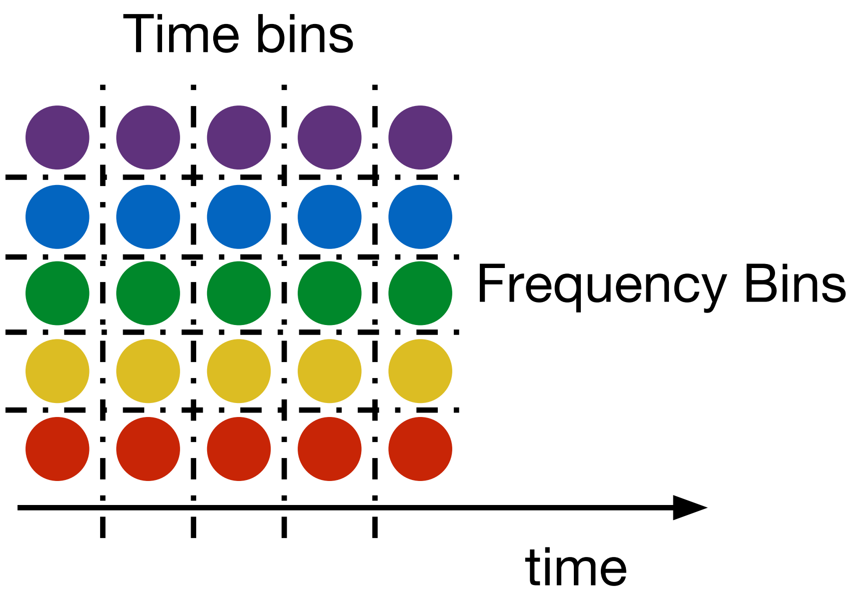
- Closed state: $\psi = \pi$
- Open state: $\psi \neq \pi$



Frequency Multiplexing



single frequency operation



frequency multiplexing

- Modified protocol
  - In each time bin, pairs at multiple frequencies are generated
  - There are many low-Q idler outputs corresponding to different frequencies
  - Generation of one photon at any frequency in any of the time bins heralds a success
  - Efficient frequency conversion at the end of the clock cycle (Li et. al. CLEO 2015)

- Increases the number of attempts at pair generation by the number of frequencies

- **Success probability >90%** can be achieved by multiplexing over 5 frequencies with the same parameters used in the single frequency operation
- Success probability > 99% appears possible assuming detection efficiency >99.5%

Producing entangled states on demand?

- 3-photon GHZ source can reduce resource requirements for cluster state quantum computing by a factor of 200
- Use an n photon creation process:

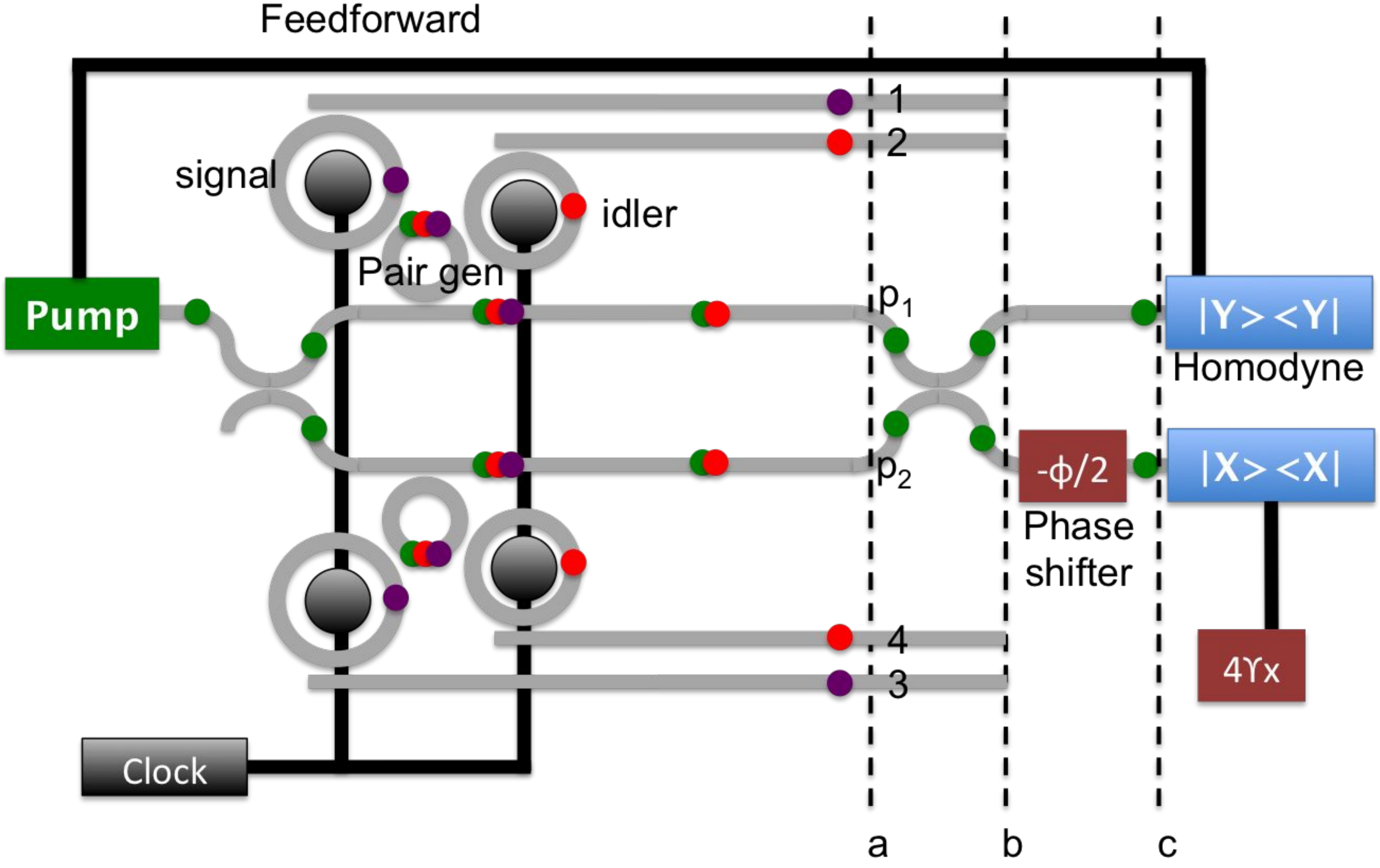
$$pump \rightarrow p_0|0\rangle^{\otimes n} + p_1|1\rangle^{\otimes n} + p_2|2\rangle^{\otimes n}$$

  - n = 2: SPDC/sFWM
  - n = 3: 3 photon down conversion with $\chi^{(3)}$
- Scramble the heralding signal from two such sources to herald without destroying entanglement
  - Method 1: QND
    - n photon GHZ from an n photon process
  - Method 2: Direct detection
    - n-1 photon GHZ from an n photon process
- Use feedback from heralding to shut off the pump: make the source deterministic

Pant et. al. (in preparation)

Method 1: QND

- Two identical sFWM sources
- The pumps go through a beam splitter before homodyne detection
- Weak nonlinearity: αθ is O(1)
  - α is the number of photons in the strong pump field
  - θ is the phase shift due to a single photon
- n photon GHZ from an n photon process



Design of a bell pair source
using sFWM
Pant et. al. (in preparation)

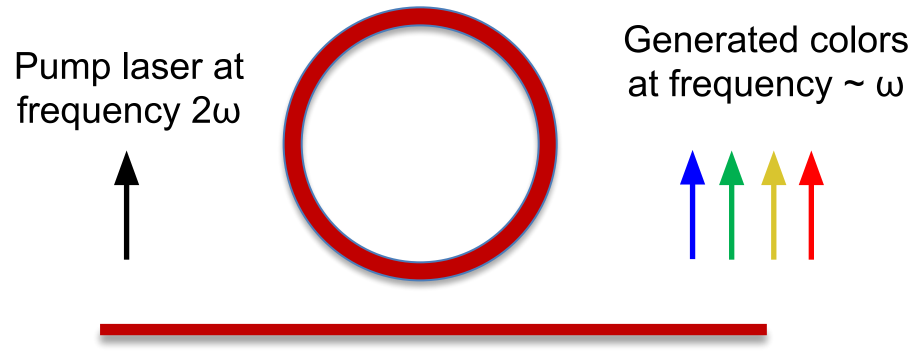
Method 2: direct detection

- n-1 photon GHZ from an n photon process
  - Requires high n

- Example: downconversion from 515 nm to 1550 band using material $\chi^{(3)}$ for the generation of dual rail bell states

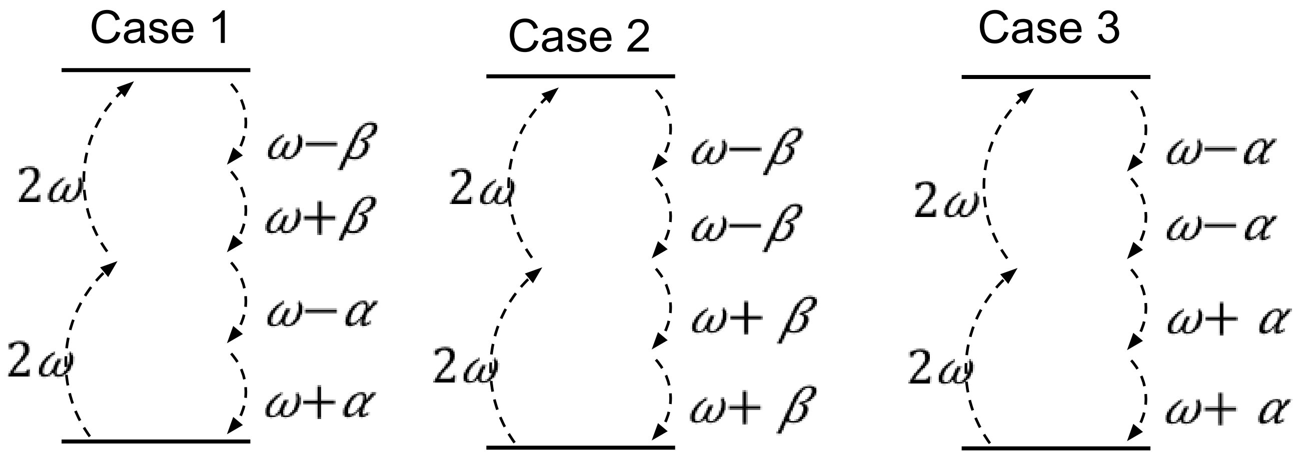
- Direct generation of 3 qubit dual rail GHZ states requires a 4 photon process

Nonlinear Six-Wave Mixing Process



- ❑ Conversion of two photon near 780 nm into 4 photons in the 1550 nm band using material $\chi^{(5)}$
- ❑ Efficiency of the process is less than SPDC or sFWM BUT The important parameter for scalable quantum computing is heralding efficiency which can be high.
- ❑ Efficiency is proportional to Q^5: High Q resonators can dramatically boost efficiency
- ❑ Our initial results show that the phase matching and anomalous dispersion required can be achieved

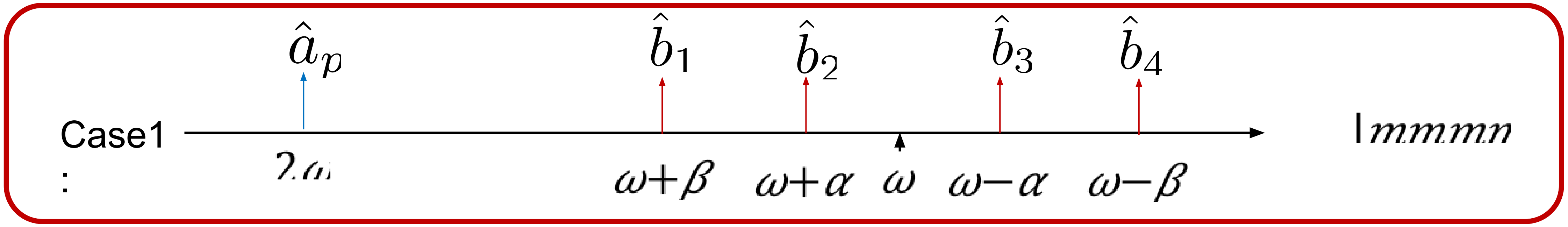
Possible cases:



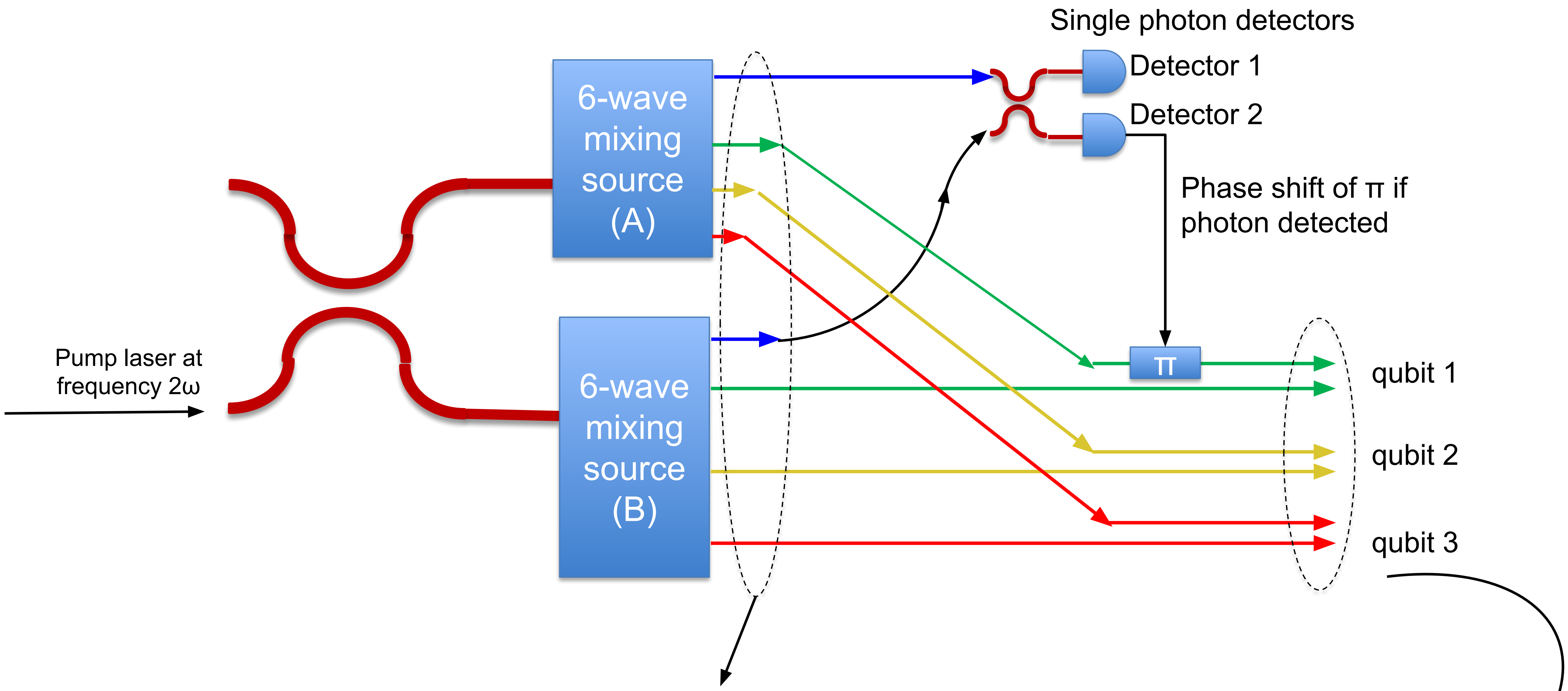
Pant et. al. (in preparation)

Case 1 is the desired case. Two ways to filter out the other cases:

- Use photon number resolved heralding. Only pick cases with one photon in the heralding mode
- The process requires phase matching and anomalous dispersion. The other processes will not meet these conditions and will be naturally suppressed.



Generation of 3 photon GHZ sources from six wave mixing sources



$$\frac{|1_{\omega-\alpha}1_{\omega-\beta}1_{\omega+\alpha}1_{\omega+\beta}\rangle_A|0_{\omega-\alpha}0_{\omega-\beta}0_{\omega+\alpha}0_{\omega+\beta}\rangle_B + |0_{\omega-\alpha}0_{\omega-\beta}0_{\omega+\alpha}0_{\omega+\beta}\rangle_A|1_{\omega-\alpha}1_{\omega-\beta}1_{\omega+\alpha}1_{\omega+\beta}\rangle_B}{\sqrt{2}}$$

$$\frac{|1_{\omega-\beta}1_{\omega+\alpha}1_{\omega+\beta}\rangle_A|0_{\omega-\beta}0_{\omega+\alpha}0_{\omega+\beta}\rangle_B + |0_{\omega-\beta}0_{\omega+\alpha}0_{\omega+\beta}\rangle_A|1_{\omega-\beta}1_{\omega+\alpha}1_{\omega+\beta}\rangle_B}{\sqrt{2}}$$

Six wave mixing vs GHZ creation from single photons

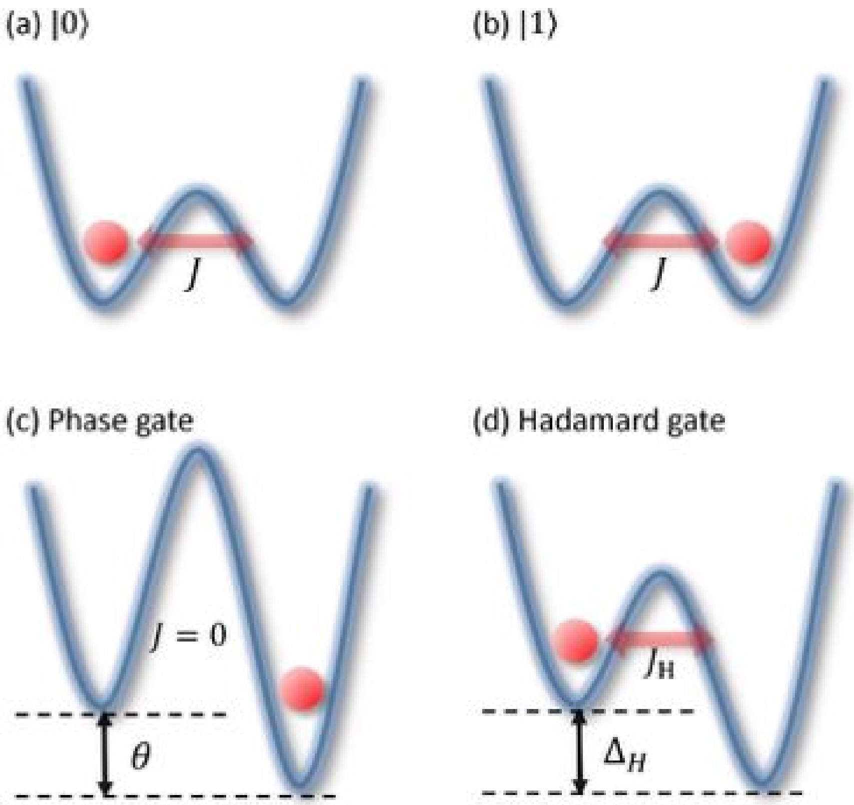
Six wave mixing will results in probabilistic, heralded creation of GHZ states. Feedforward on the heralding signal is required to make the source deterministic

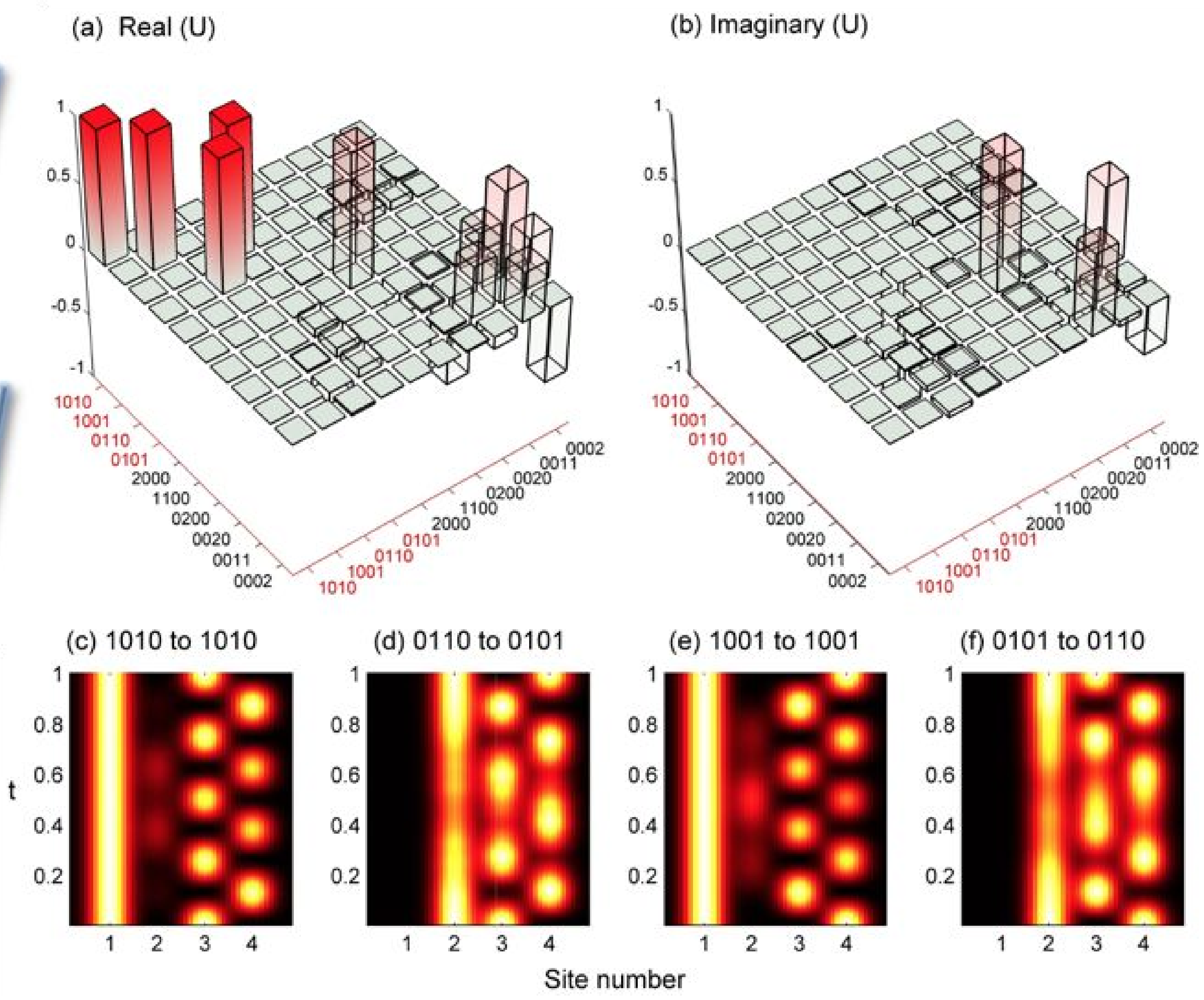
Why is this better than probabilistic generation of single photons from SPDC followed by postselected linear optics?

	SPDC/sFWM->Single photons ->postselected linear optics -> GHZ	Six wave mixing -> GHZ
Average number of attempts	**128**	**10.3**
Number of Feedforward steps	**2**	**1**

Six wave reduces resource requirements and feedforward!

Deterministic Gates with Interacting Bosons



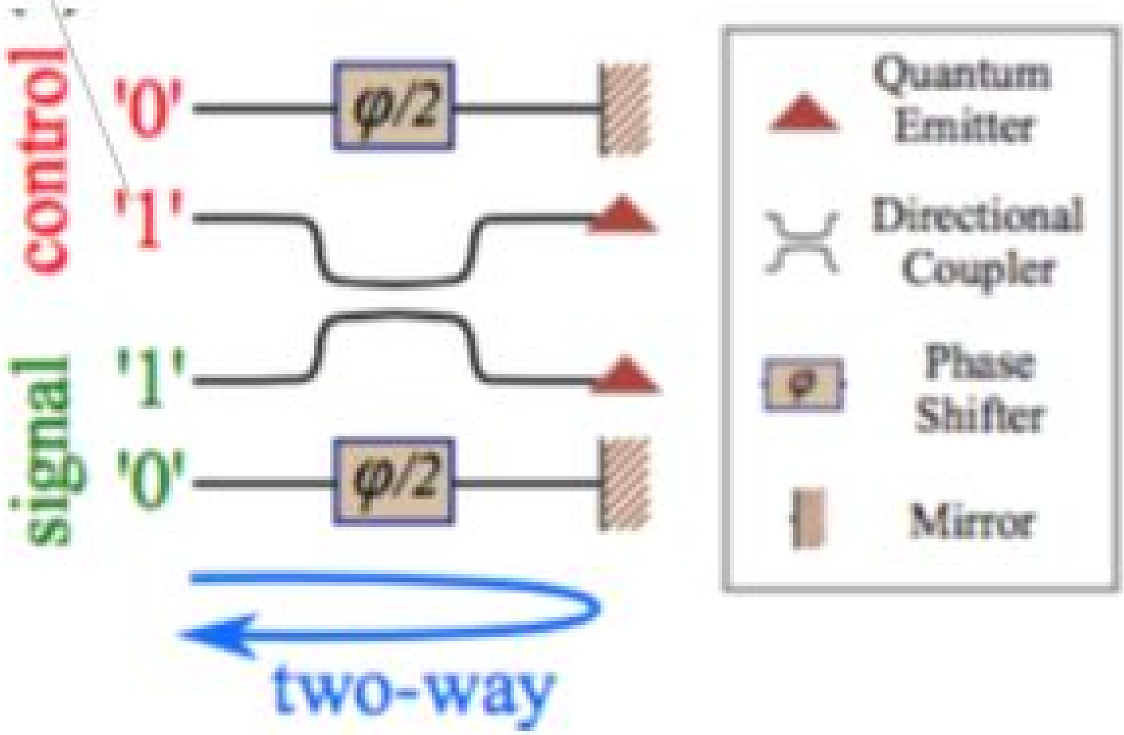


Lahini, Y., Steinbrecher, G. R., Bookatz, A. D., & Englund, D. (2015). arXiv:1501.04349.

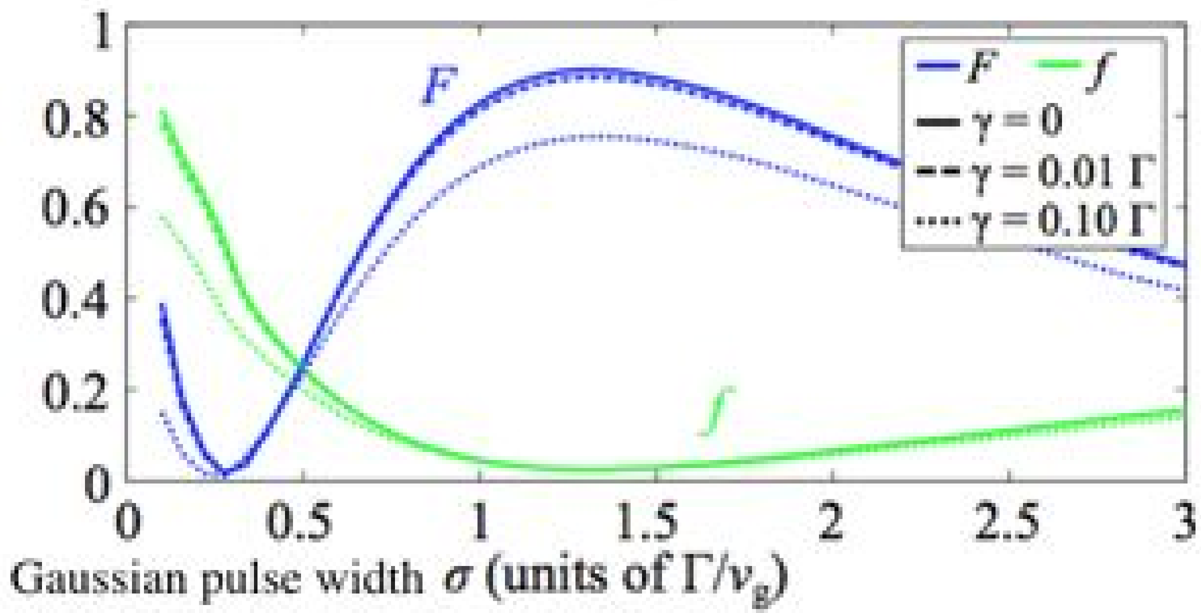
Proposal for 2-photon nonlinear gate

$$|\bar{1}_c\rangle = \int_{-\infty}^{\infty} \mathrm{d}k\, \xi(k)t(k)\, a^{\dagger}_{1c}(k)|\phi\rangle$$

Scattered two-photon state fidelity compared to the ideal state $-|\bar{1}_c\rangle|\bar{1}_s\rangle$



F=fidelity, f=phase measure (f=0: ideal)



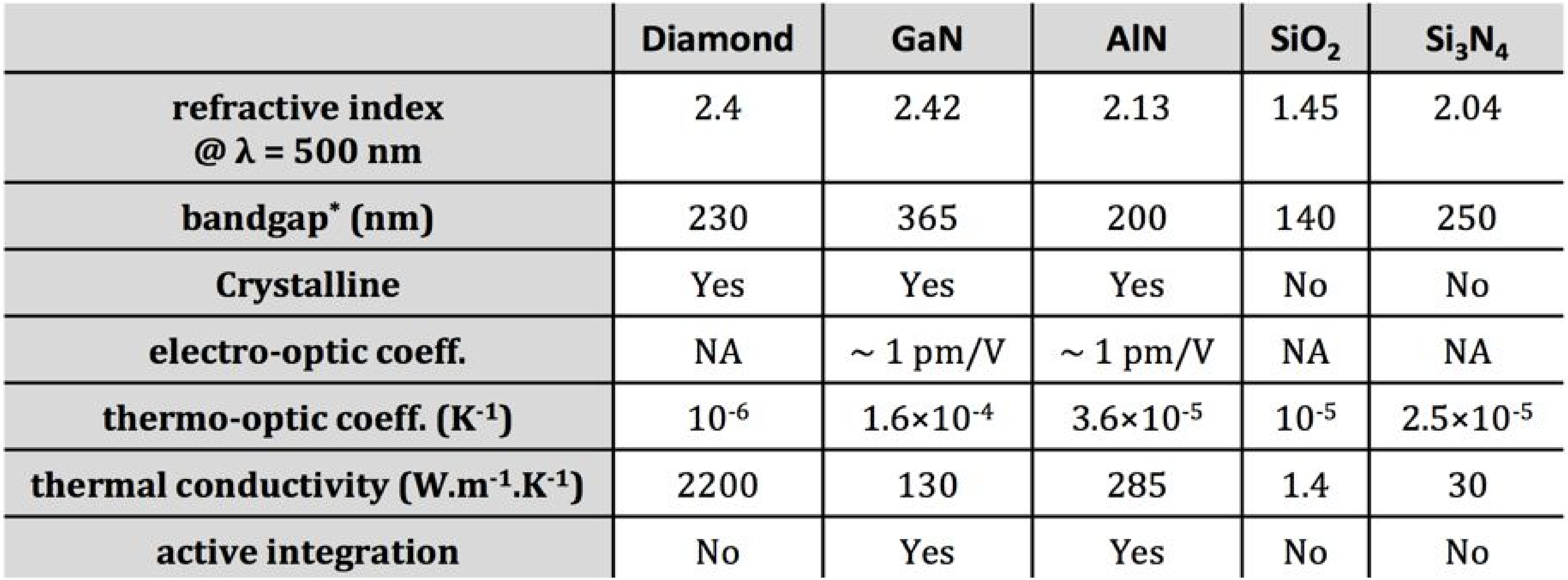
Example: For semiconductor quantum dot in PC waveguide,
$\Gamma/(\gamma + \Gamma) = 0.98$ ==> F ~ 90 %.

- Anders Nysteen, Mikkel Heuck, Dara P. S. McCutcheon, Jesper Mørk, and Dirk R. Englund, Proposal for a passive two-photon controlled-phase gate using intrinsic non-linearities of two-level emitters, to be submitted (2016)

- Full set of quantum logic gates in coupled resonators under Bose-Hubbard Hamiltonian:

High-fidelity Quantum Logic Gates with Interacting Bosons on a 1D Lattice, Yoav Lahini, Gregory R. Steinbrecher, Adam D. Bookatz, Dirk Englund, arXiv:1501.04349 (2015)

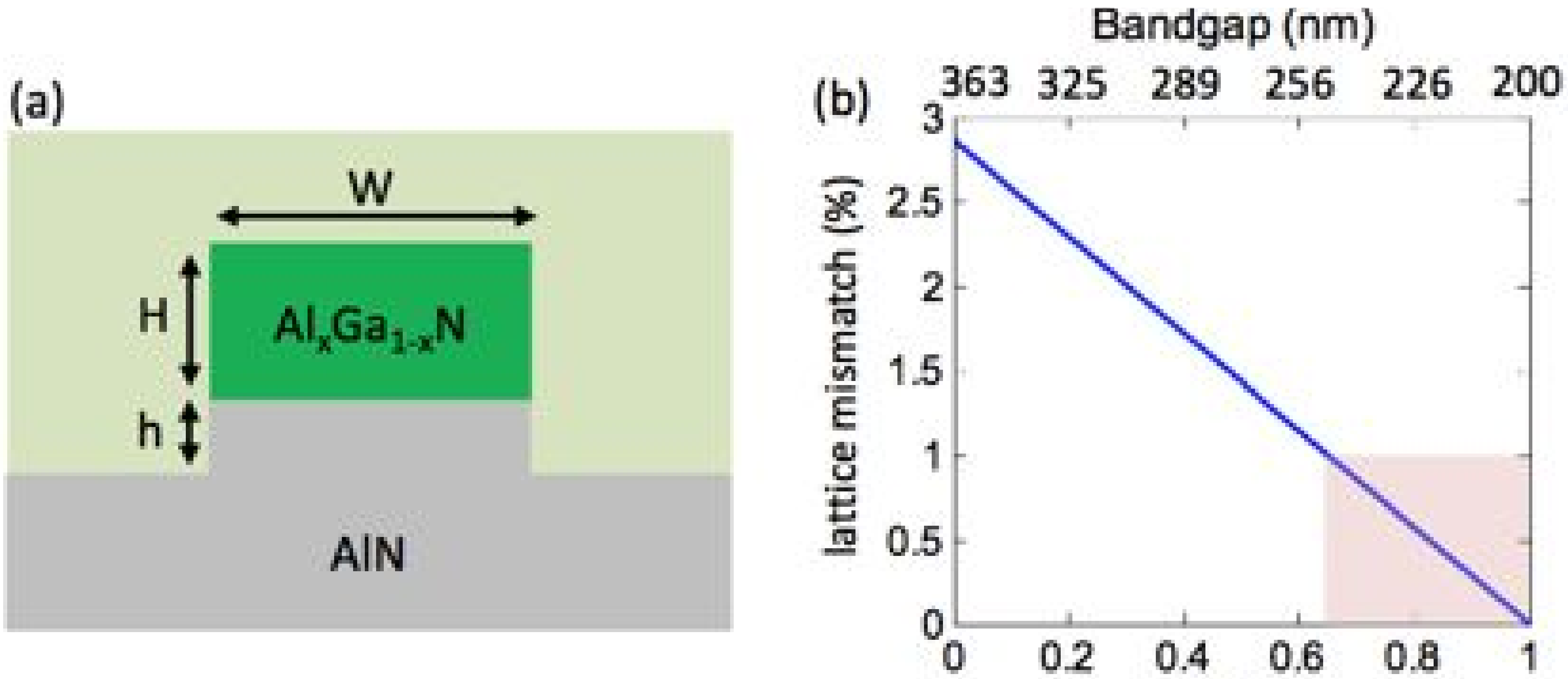
Other Photonics Platforms



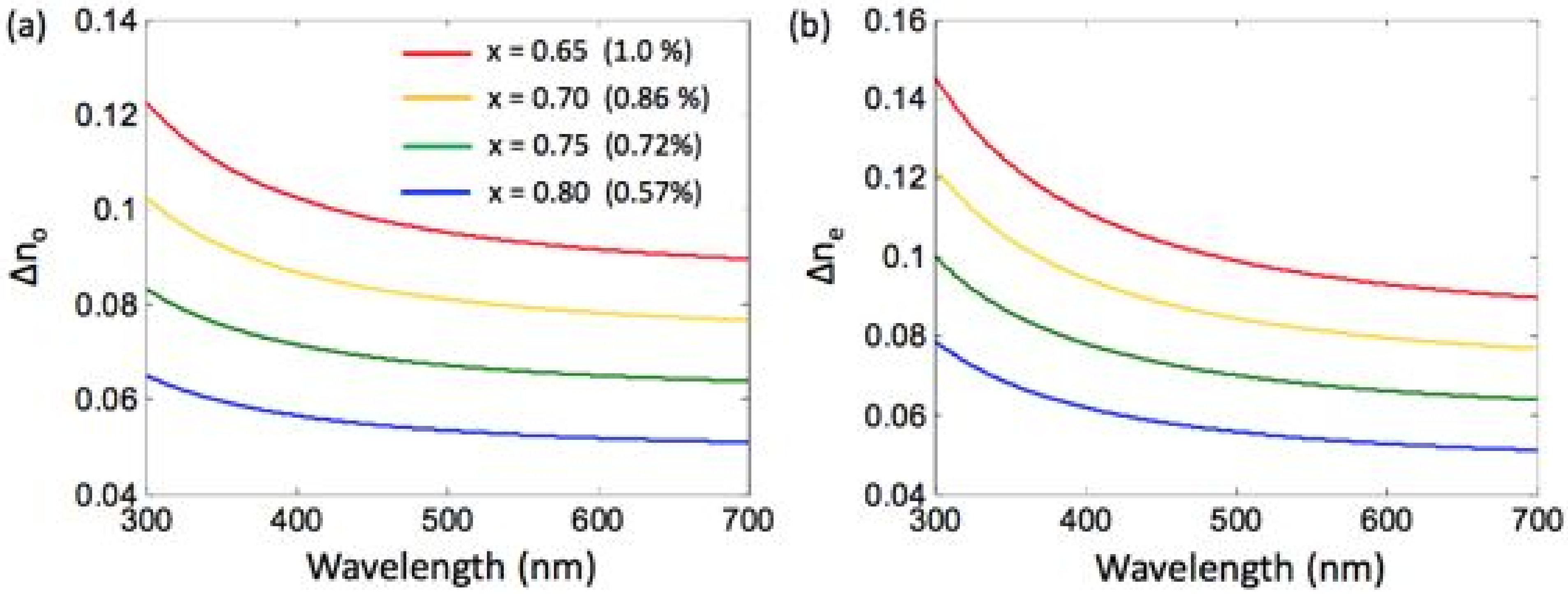
	Diamond	GaN	AlN	SiO_2	Si_3N_4
refractive index @ λ = 500 nm	2.4	2.42	2.13	1.45	2.04
bandgap* (nm)	230	365	200	140	250
Crystalline	Yes	Yes	Yes	No	No
electro-optic coeff.	NA	~ 1 pm/V	~ 1 pm/V	NA	NA
thermo-optic coeff. (K^{-1})	10^{-6}	1.6×10^{-4}	3.6×10^{-5}	10^{-5}	2.5×10^{-5}
thermal conductivity ($W.m^{-1}.K^{-1}$)	2200	130	285	1.4	30
active integration	No	Yes	Yes	No	No

AlGaN Wide-Bandgap Photonics

Mohammad Soltani, Richard Soref, Dirk Englund



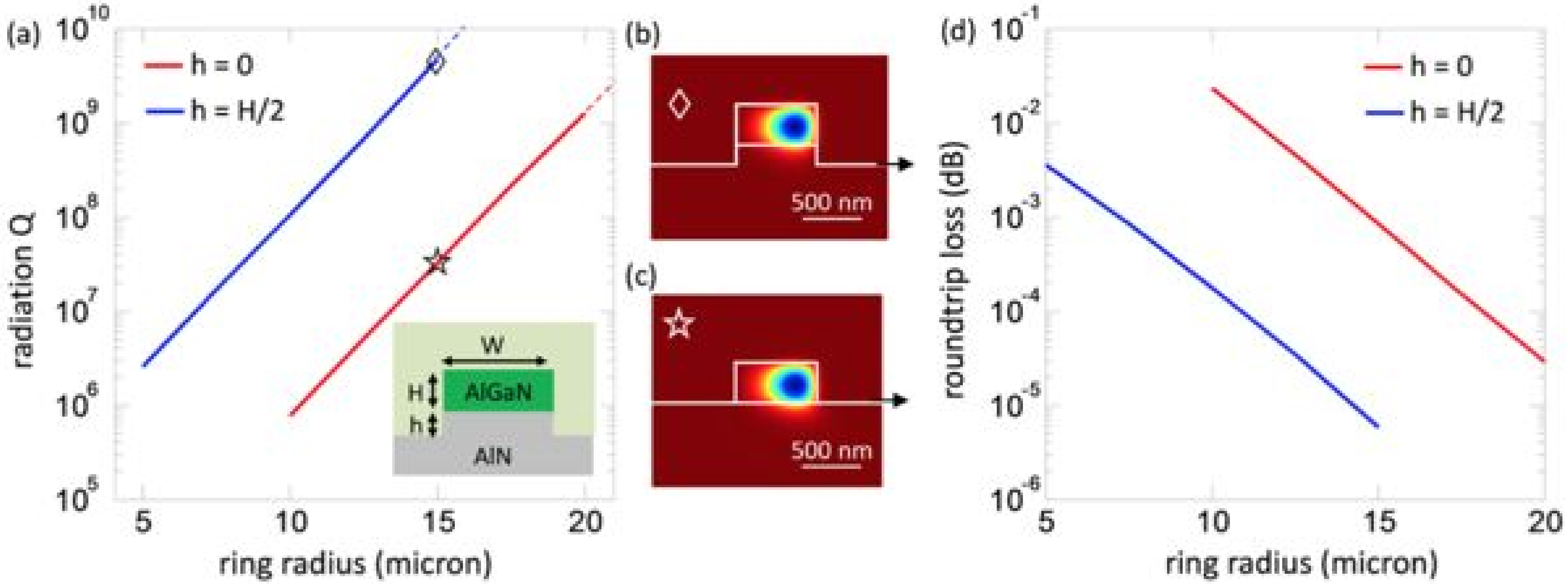
(a) Cross section of the AlxGa1-xN waveguide. (b) Variation of AlxGa1- xN/AlN lattice-mismatch vs. x. The top horizontal axis shows the bandgap of AlxGa1-xN in the wavelength unit for the each x value.



Refractive index difference between the AlxGa1-xN and AlN for (a) ordinary and (b) extraordinary indices with the x values and lattice mismatches shown in the inset of (a).

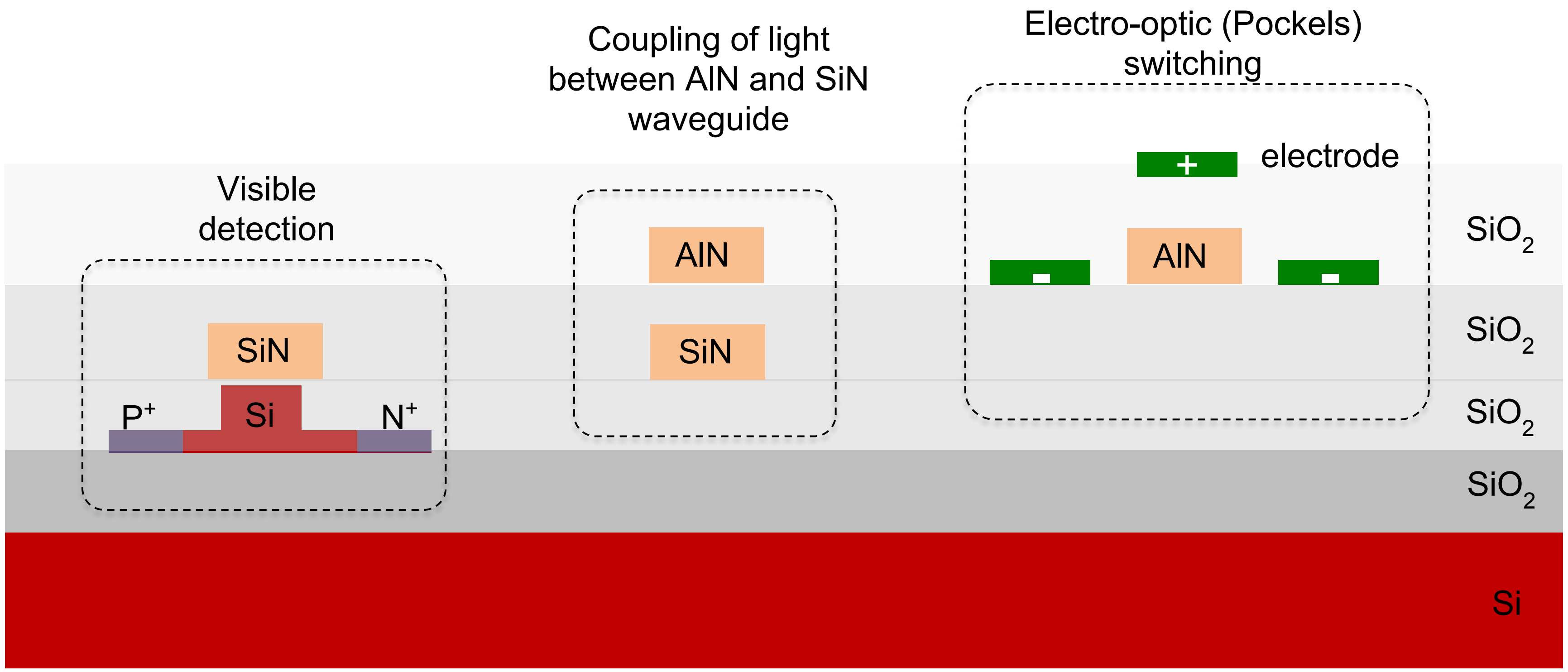
Design study

AlGaN Photonics



(a) Simulated radiation Q for the TE mode of an Al0.65Ga0.35N ring resonator vs. its radius for a resonance wavelength ~ 300 nm and for h = 0 and h = H/2. The inset shows the ring cross section. For this simulation W = 700 nm, H = 350 nm. (b)-(c) Cross section of the radial electric field mode profiles for a ring radius of 15 microns for h = H/2 and h = 0, respectively. (d) Roundtrip loss of the rings in (a).

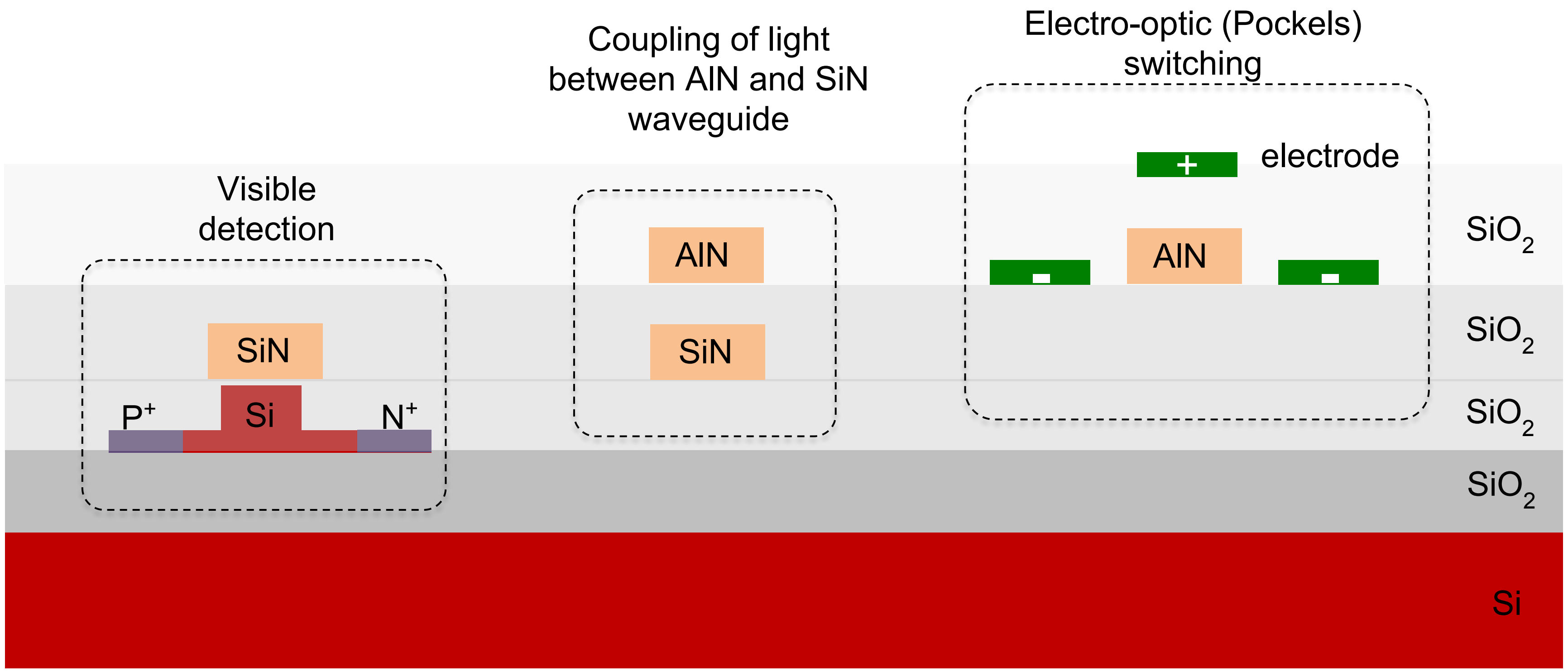
Monolithic Visible-to-IR Quantum Photonic Fabrication on a Foundry Si platform


Coupling of light between AlN and SiN waveguide
Electro-optic (Pockels) switching
Visible detection
+
electrode
-
-
AlN
AlN
SiN
SiN
P+
Si
N+
SiO2
SiO2
SiO2
SiO2
Si

A path to all the required operations on the same integrated photonics platform (through AIM Photonics, SUNY Fab)

- Fast low-loss modulation for feed-forward in AlN using pockels effect
- Efficient detection in Si
- Broadband nonlinear optics for generation of a variety of heralded sources in SiN ($\chi^{(3)}$ and $\chi^{(5)}$) and AlN ($\chi^{(2)}$)
- Compatibility with SNSPD integration.

Monolithic Visible-to-IR Quantum Photonic Fabrication on a Foundry Si platform


Coupling of light between AlN and SiN waveguide
Electro-optic (Pockels) switching
electrode
+
-
-
AlN
AlN
SiN
SiN
Visible detection
P+
Si
N+
SiO2
SiO2
SiO2
SiO2
Si

A path to all the required operations on the same integrated photonics platform (through AIM Photonics, SUNY Fab)

- Fast low-loss modulation for feed-forward in AlN using pockels effect
- Efficient detection in Si
- Broadband nonlinear optics for generation of a variety of heralded sources in SiN ($\chi^{(3)}$ and $\chi^{(5)}$) and AlN ($\chi^{(2)}$)
- Compatibility with SNSPD integration.

Getting photons under control

Photonic qubits are out of control!

Capture them in resonators

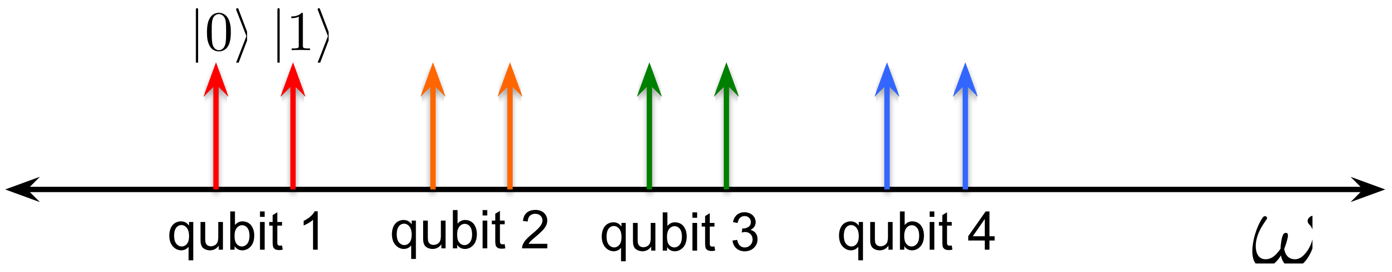
- Interactions by detection
- Interactions by nonlinearity

→ Closely analogous to SCQC in the optical domain!

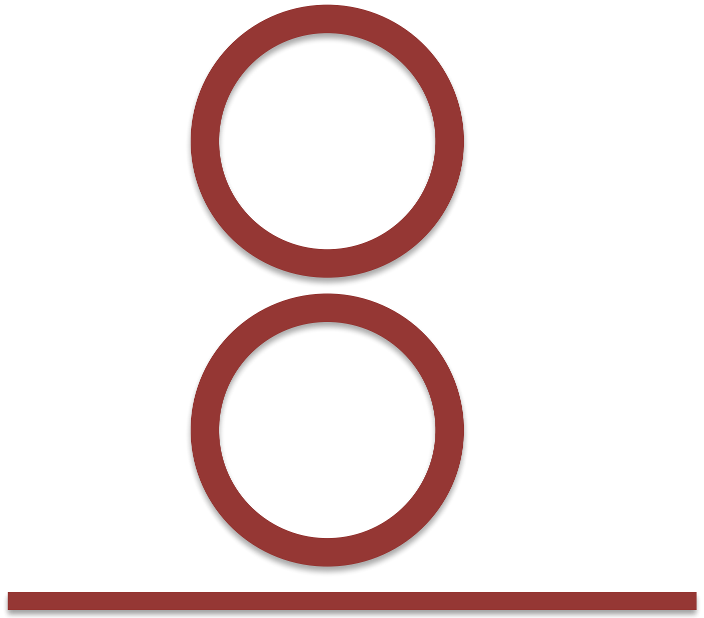
Intermediate devices/spin-offs are already important!

- Example: on-demand entangled pair sources would solve the arguably biggest hurdle in quantum networking with rare earth ions and atomic gases

Ising model solver based on Quantum Annealing



Frequency encoded dual rail qubits

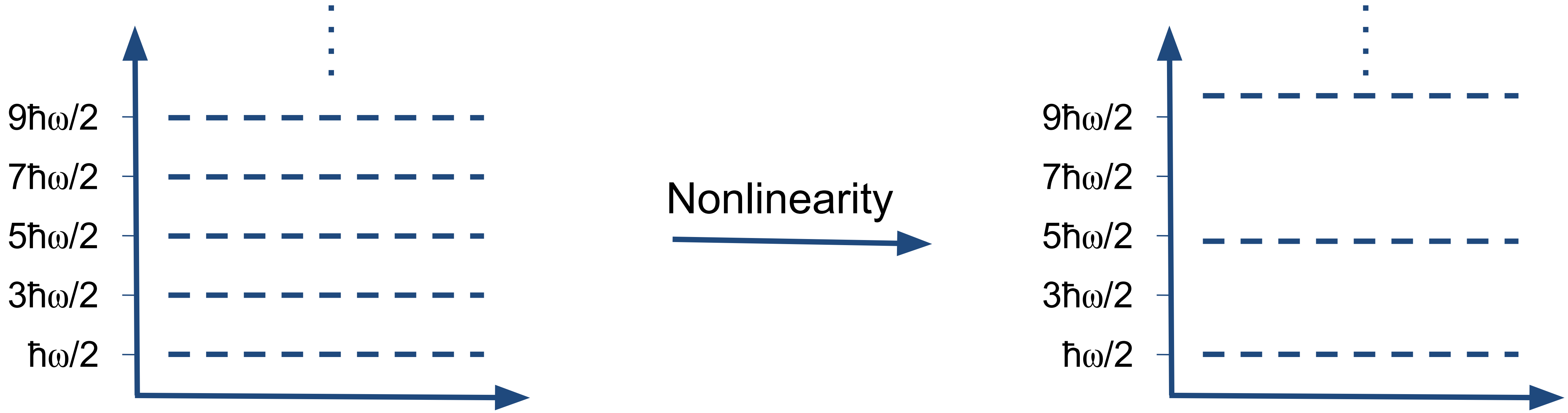


Photonic Molecule

- Photon creation: sFWM in the ring. Temporal multiplexing in high Q ring for near deterministic creation.
- Single qubit beam-splitter: Frequency conversion by ring modulation or Bragg scattering FWM
- Single Qubit Phase: Phase on a single qubit can be imparted by interaction with a classical pump mode with cross-kerr interaction.
- Two qubit phase gates: The modes will interact due to cross kerr nonlinearity in the ring which will be enhanced due to the high Q of the rings.
- The single and two qubit phase gates can be tuned up linearly in time by increasing the interaction time between single qubit beam-splitter operations i.e. by changing the time spent in each step.

Hundreds of qubits in a ring. Minimal interaction of light outside the ring allows for higher Q.

A nonlinear quantum computing architecture inspired by superconducting QC



- High Q ring resonators can allow splitting of the energy levels similar to superconducting systems
- Optical qubits offer several advantages over superconducting qubits

Microwave vs optical photon QC

	Superconducting qubits	Optical qubits
Coherence time (T1 & T2)	~ 100s of μs	~ 100s of μs
Carrier frequency (Hz)	$\sim 10^{9}$	$\sim 10^{14}$
Qubit area (μm^2)	10^{4}	10
Operating temperature for ~ zero thermal photons	10s of mK	Room temp
Nonlinearity: $\Delta\omega_{\text{single photon}}/\kappa$	$\sim 10^{2}$	In-line: Assume $n_2 \sim 10^{-12} cm^2/W$ for GaAs. For one photon in PhC cav ($V_m \sim 0.1\ (\lambda/n)^3$), $\Delta n \sim 10^{-7}$; for polymer (assume $n_2 \sim 10^{-7} cm^2/W$) and fractal cavity ($V_m \sim 0.01\ (\lambda/n)^3$, we get

Strong coupling cavity

SNSPD: detailed slides

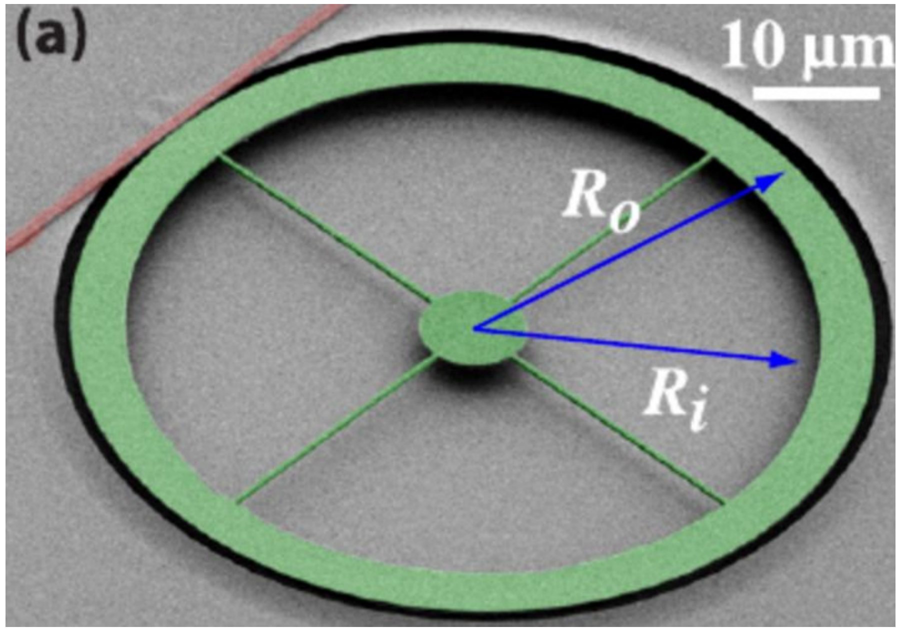
SNSPD-related tasks

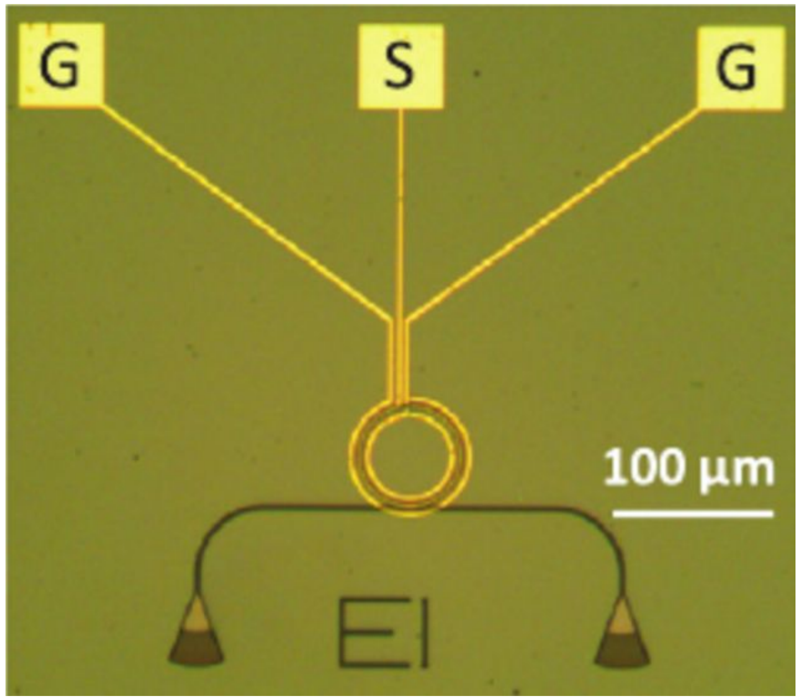
1. Fabricate 64 functioning single-photon detectors on PIC with > 90 % efficiency
2. Investigate on-chip schematic for 64 detectors parallel read-out .
3. Implement 64-channel fiber-coupled off-chip detector system.

Aluminum Nitride for integrated photonics

- Large bandgap (6.23 eV @ 77K)
  - Transparent from 200 nm to 10 µm
  - Low fluorescence
- Piezoelectric & electro-optic effect
  - Optical modulator for feedforward operation

Require compatible fabrication processes for SNSPDs !

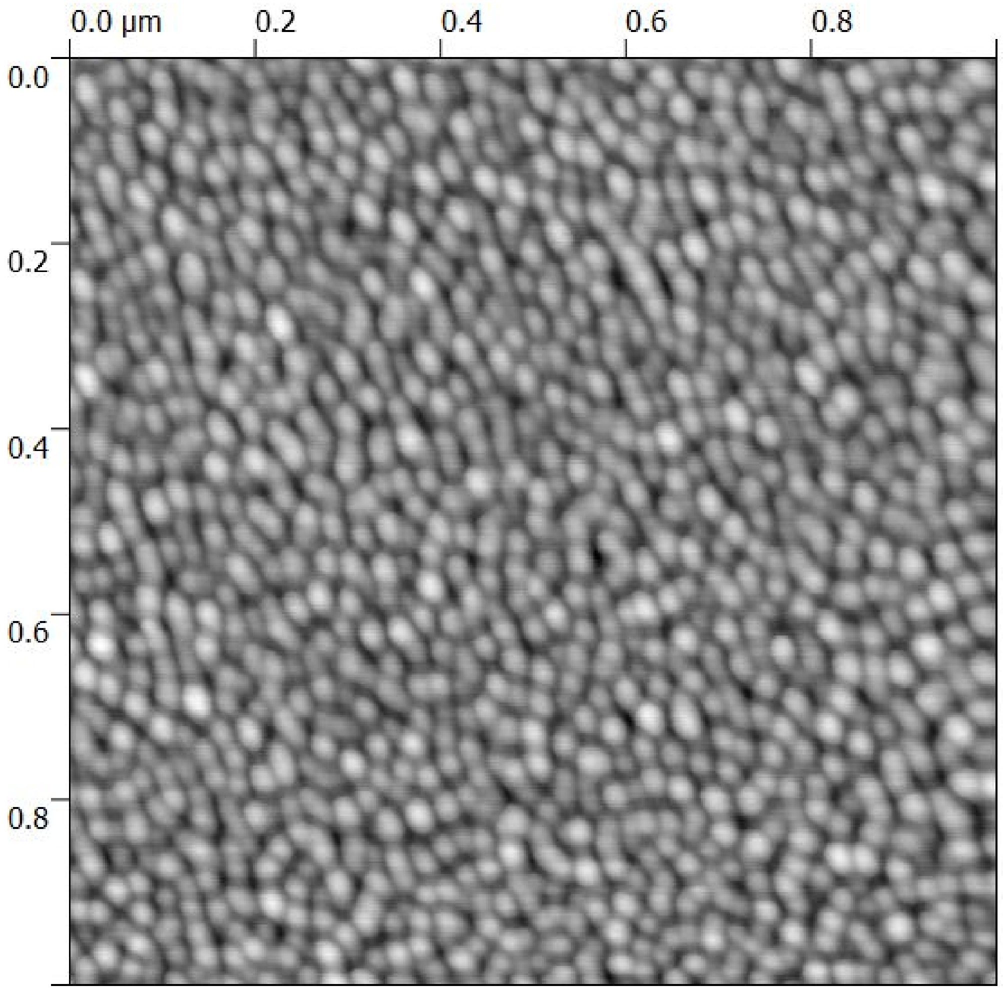




Xiong et al., New Journal of Physics (2012)

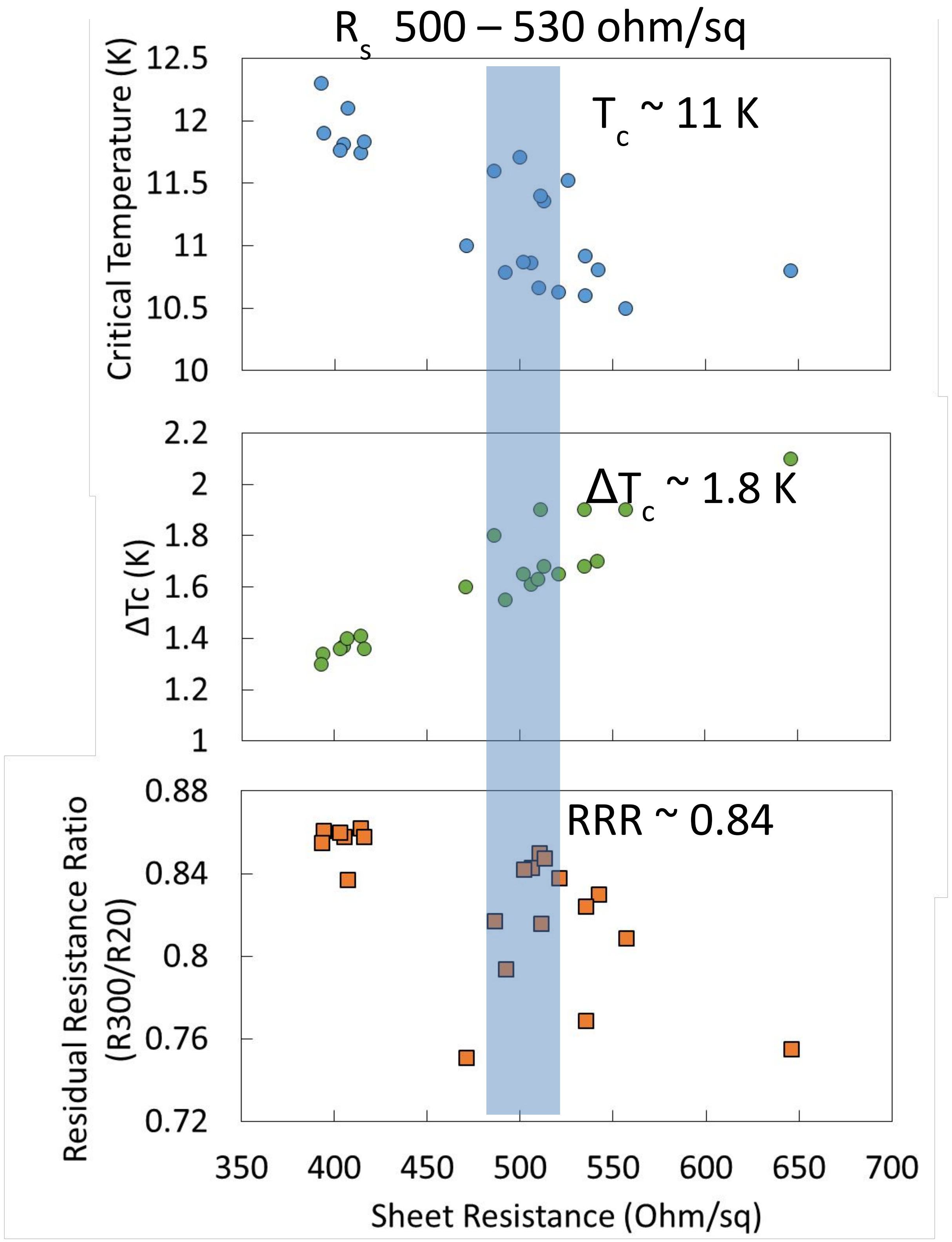
High quality NbN films on AlN

- 200 nm AlN on sapphire substrate
- Reactive DC magnetron sputtering @ 840 DegC



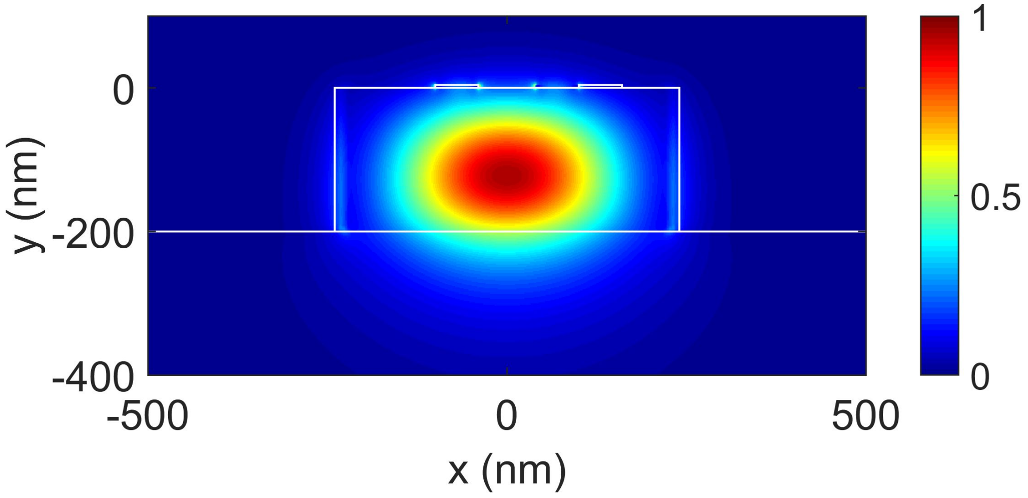
RMS roughness: 0.456 nm

Thickness: ~ 4.8 nm

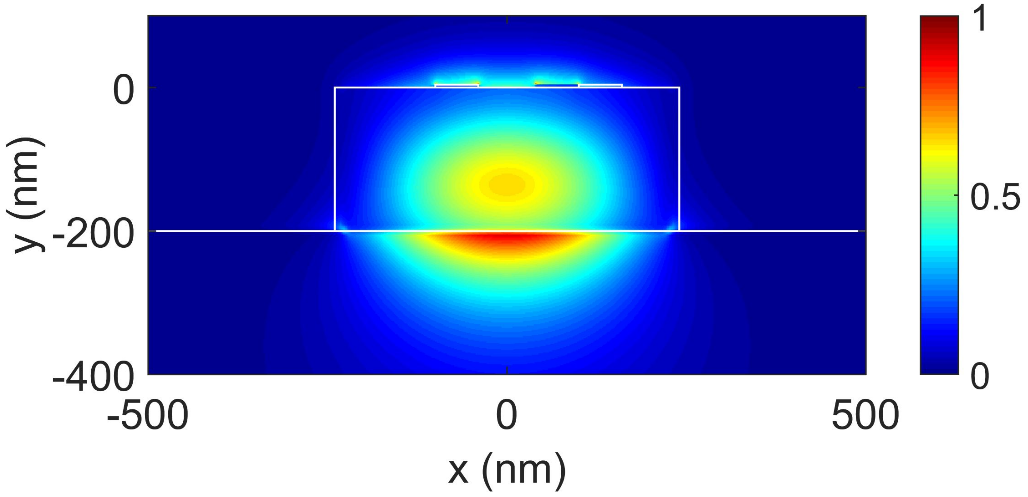


Absorbance of waveguide coupled SNSPD

Single mode ridge waveguide (450 nm × 200 nm)



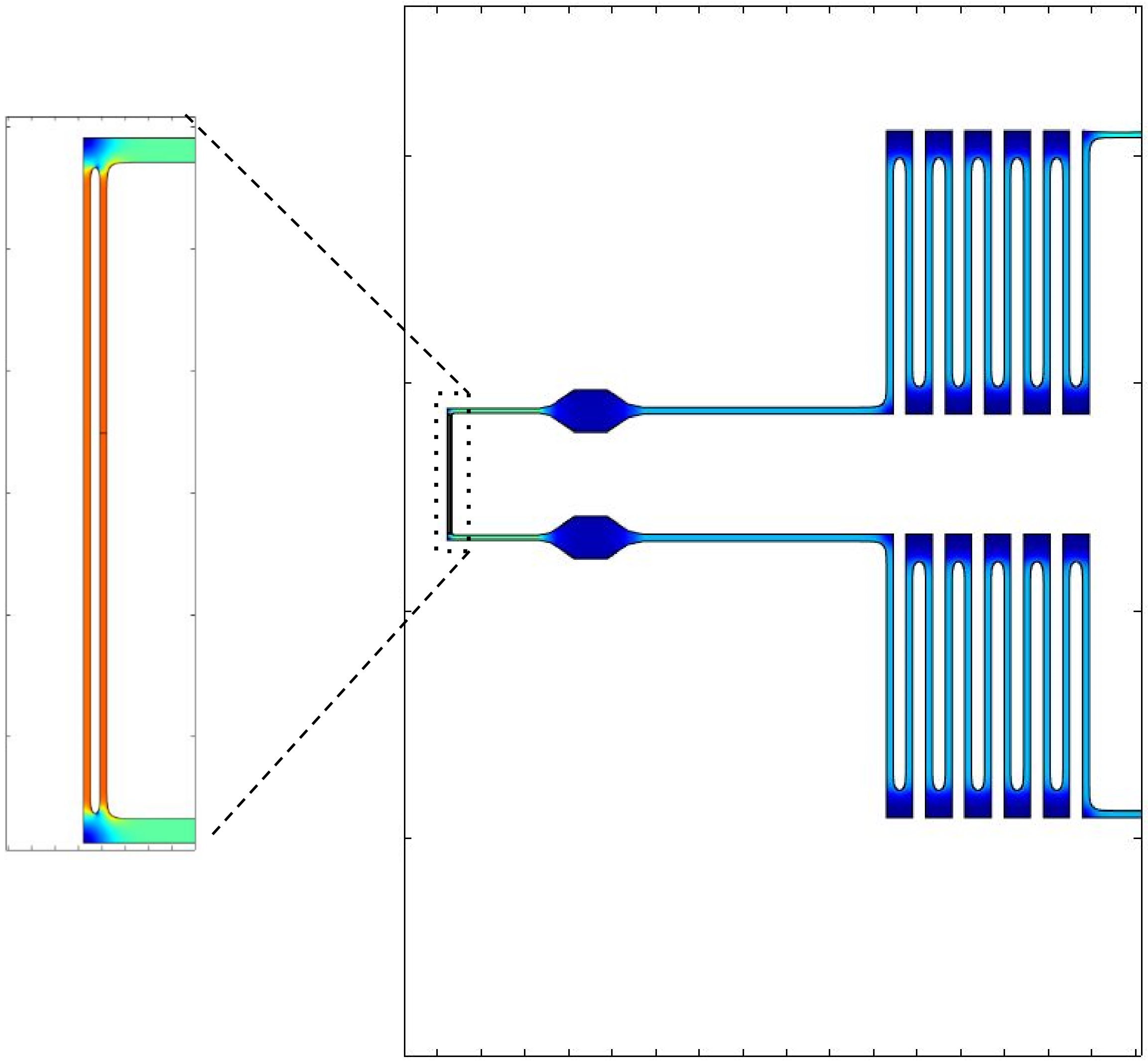
TE: $n_{\mathrm{eff}} = 1.83 + 7.52\times10^{-3}i$
Absorption: **0.64 dB/µm**

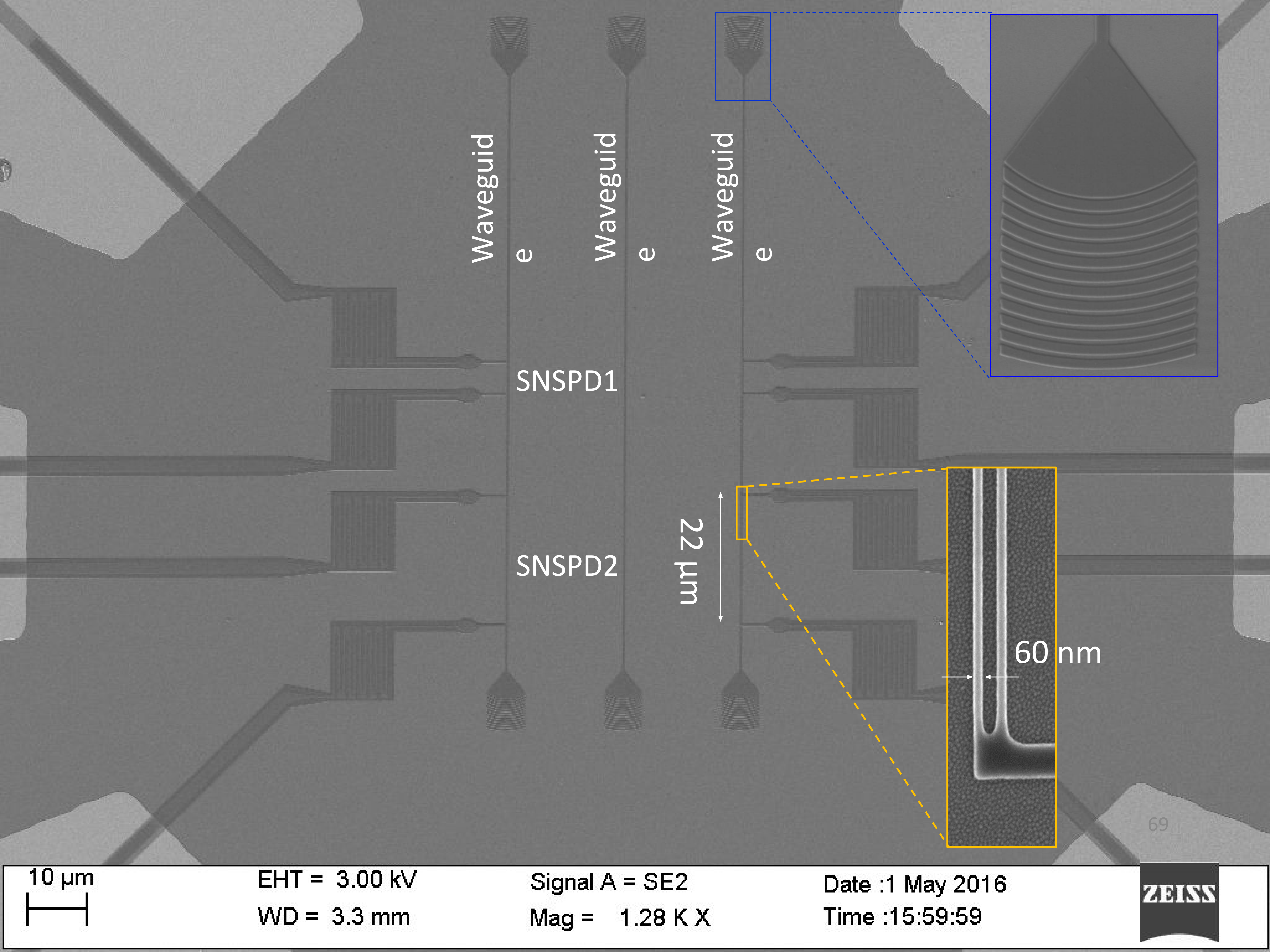


TM: $n_{\mathrm{eff}} = 1.779 + 6.31\times10^{-3}i$
Absorption: **0.55 dB/µm**

Tuning detection efficiency to achieve correlation measurements on chip

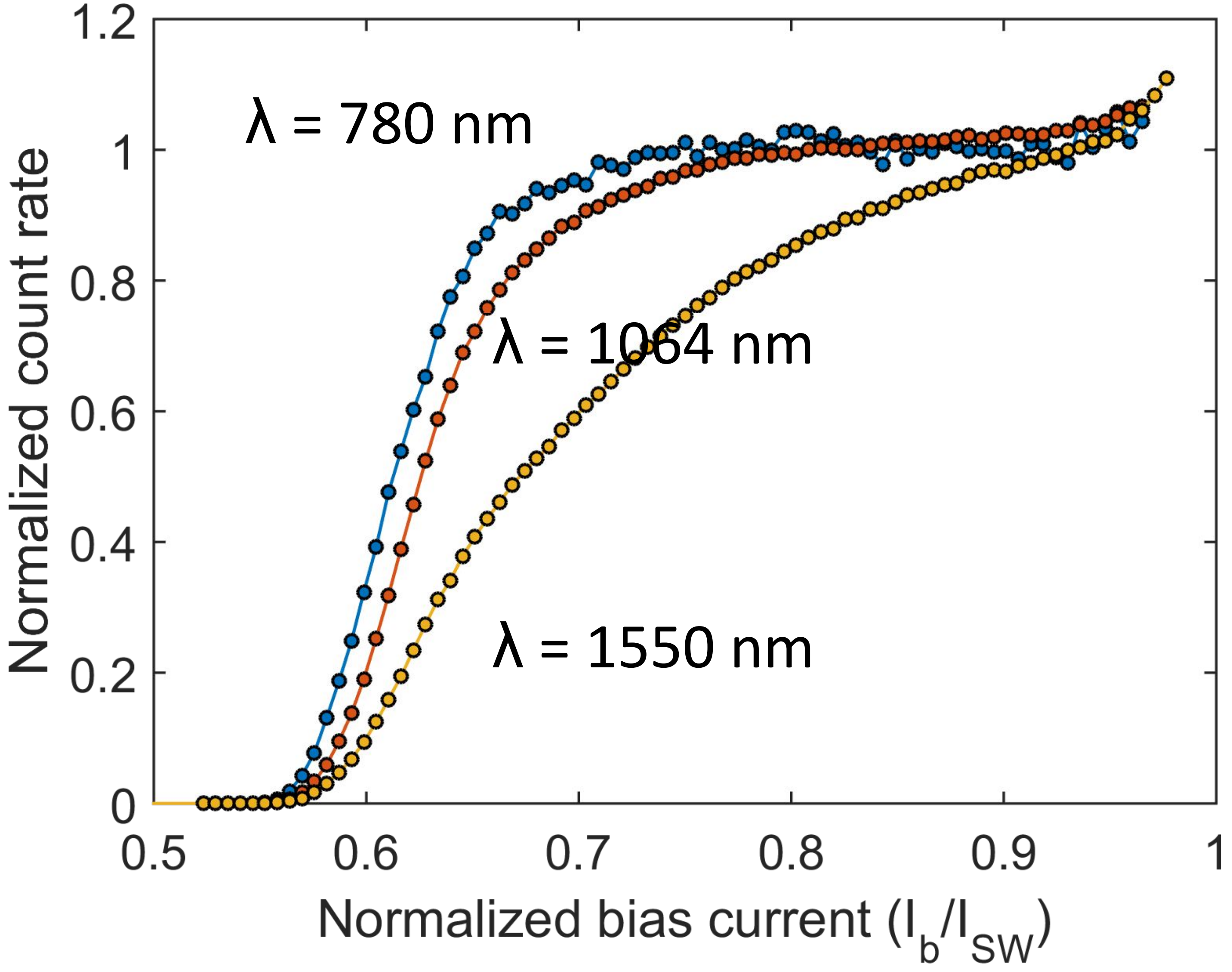
50% absorption: **5 µm**, 95% absorption: **21.7 µm**

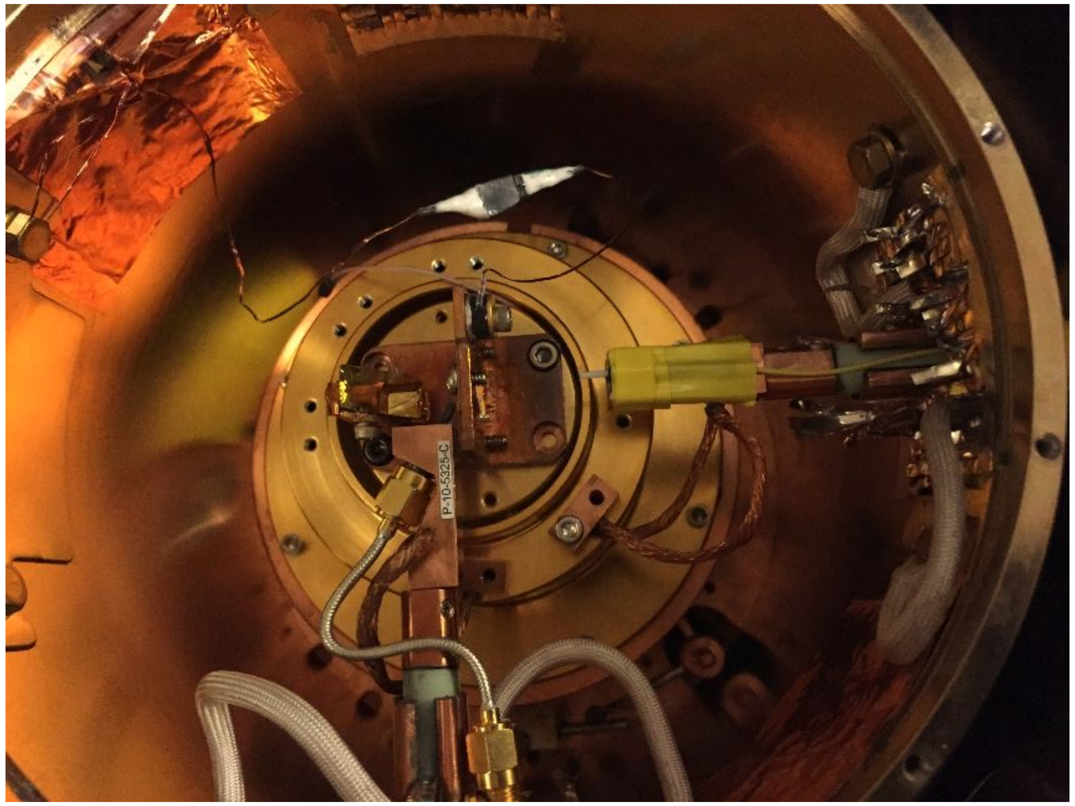



Waveguid e
Waveguid e
Waveguid e
SNSPD1
SNSPD2
22 µm
60 nm
10 µm
EHT = 3.00 kV
WD = 3.3 mm
Signal A = SE2
Mag = 1.28 K X
Date :1 May 2016
Time :15:59:59
ZEISS

Characterizations of the detectors

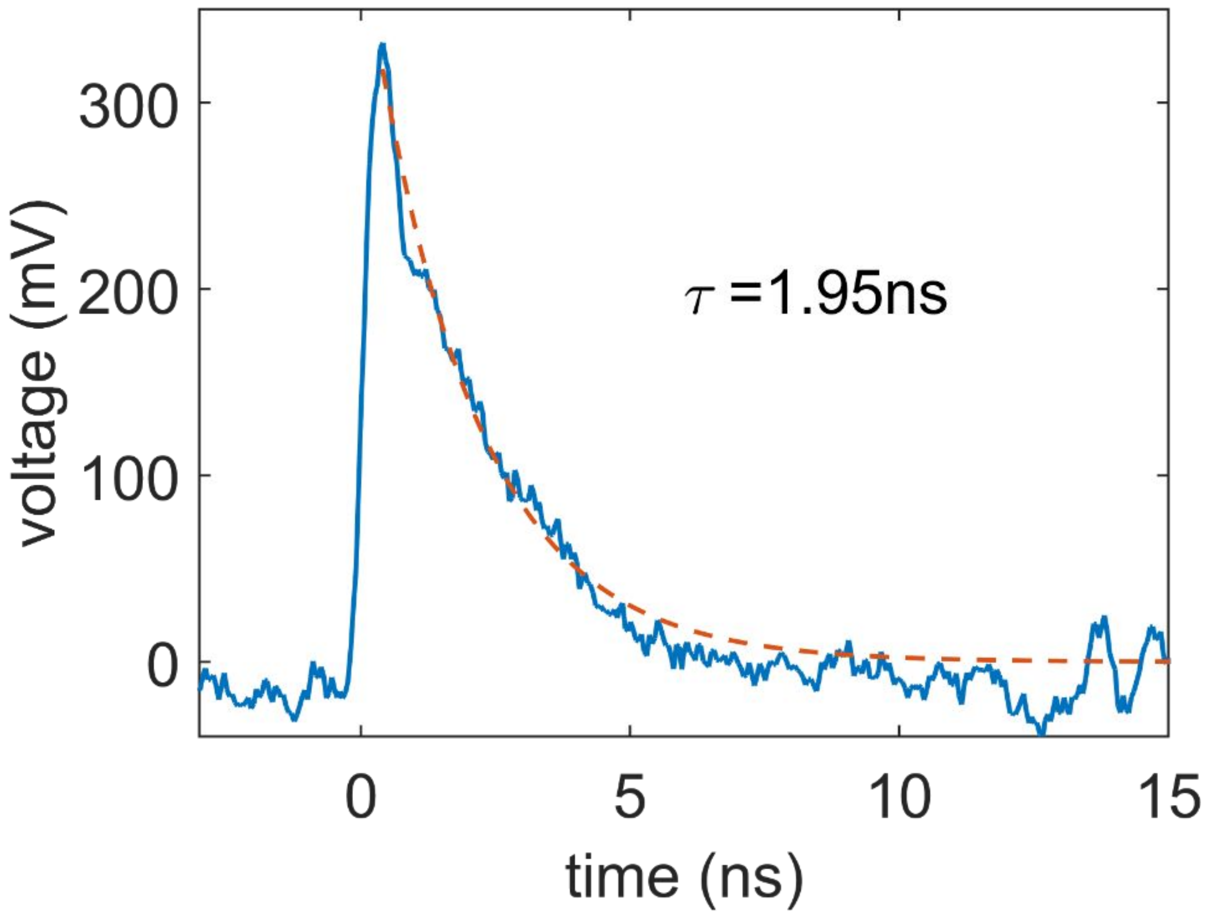
Saturated detection efficiency



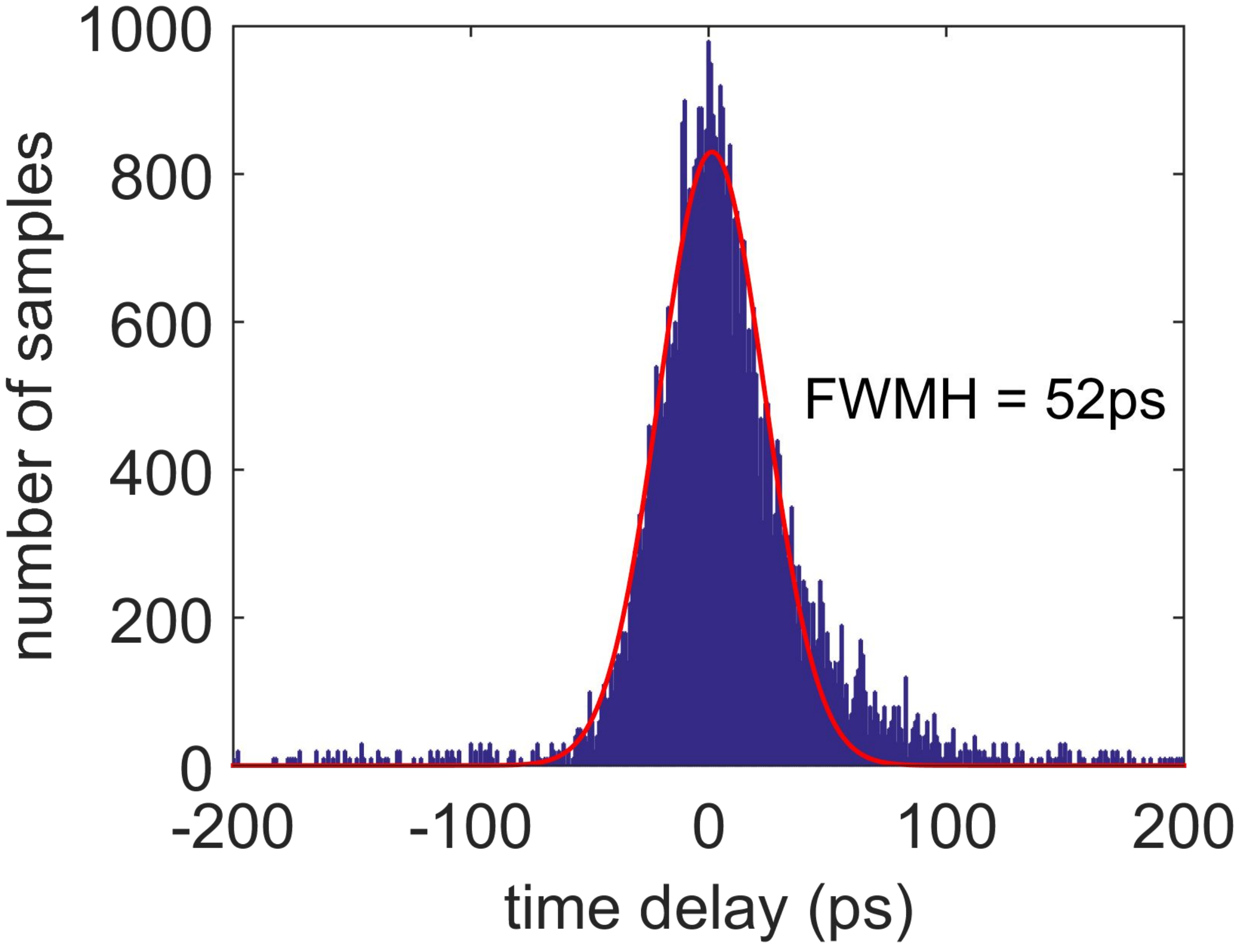


- 2.5 K cryogenic probe station
- Back illumination
- Saturation indicates high quantum efficiency

Detector timing performance

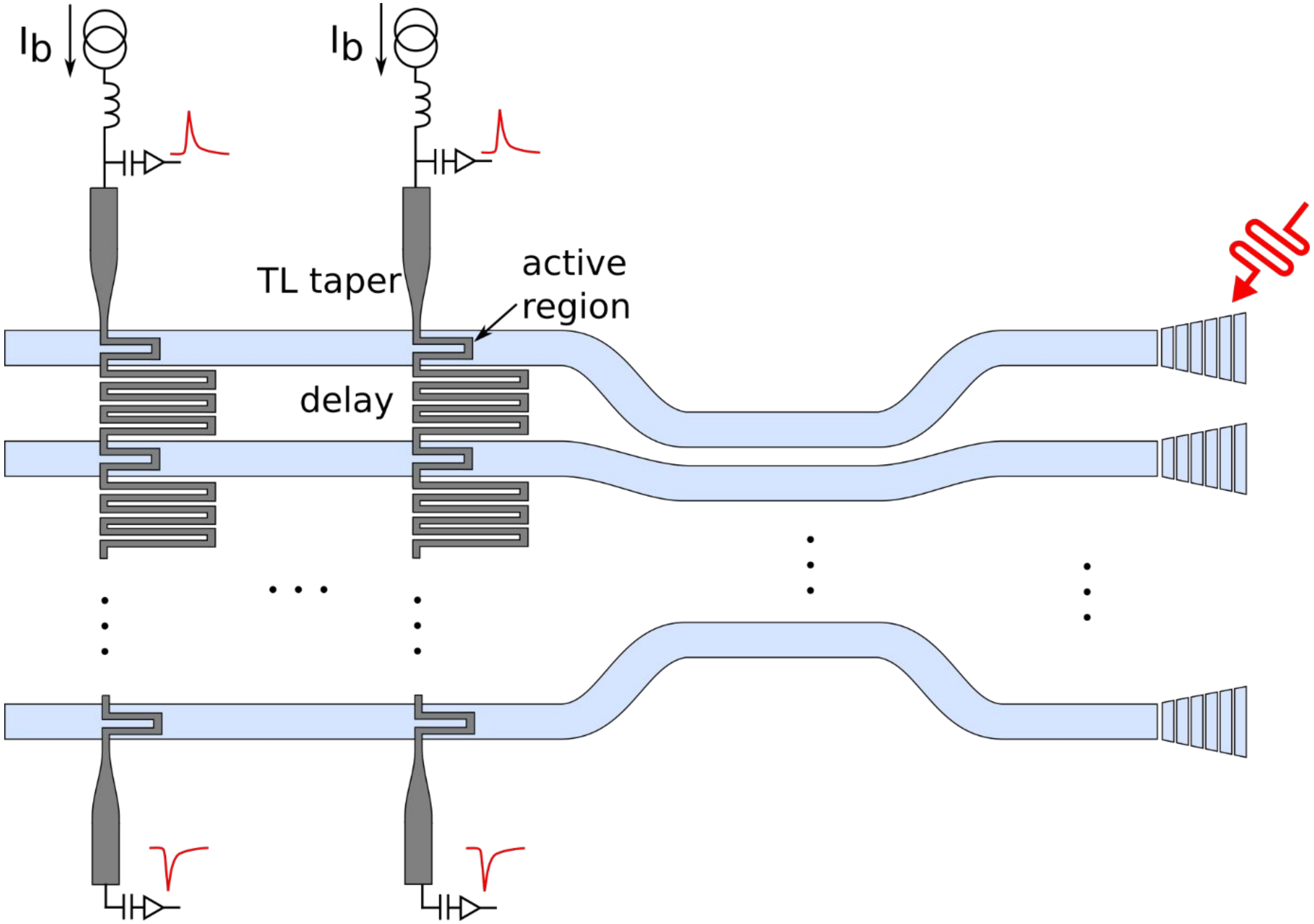


~ 6 ns reset time



52 ps timing jitter

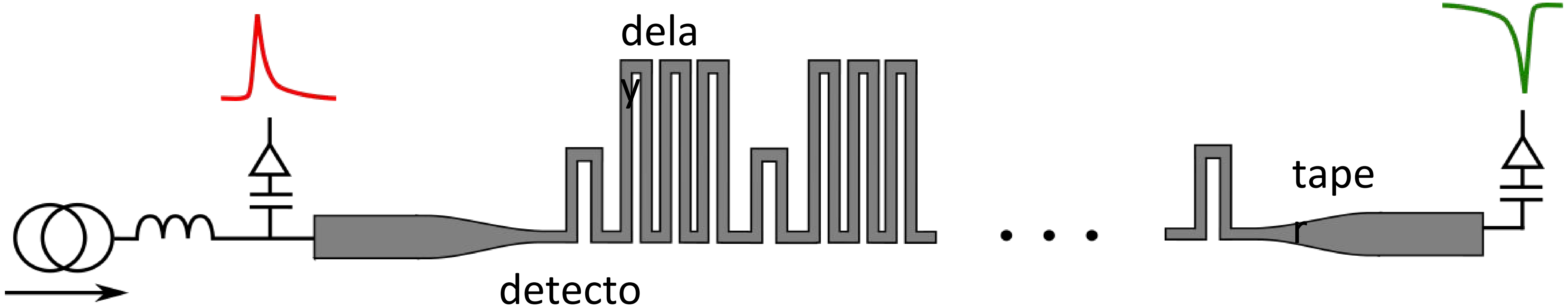
Scalable integration of 64 detectors on PIC



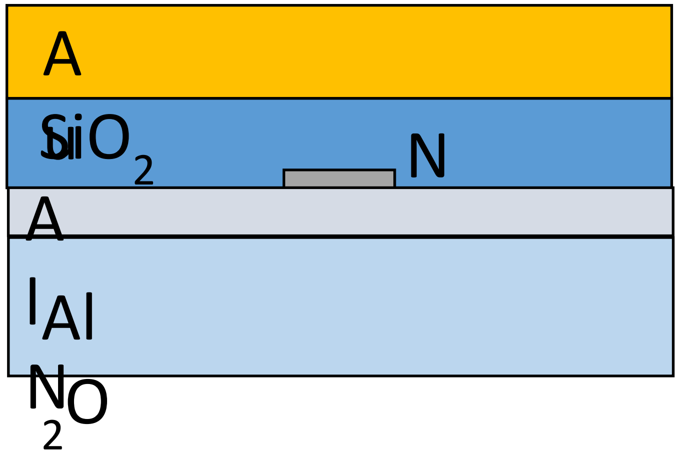
Impedance matched readout of 4 detector chains

Each chain consists of 16 detectors, all integrated on AlN waveguide

Key components in a detector chain

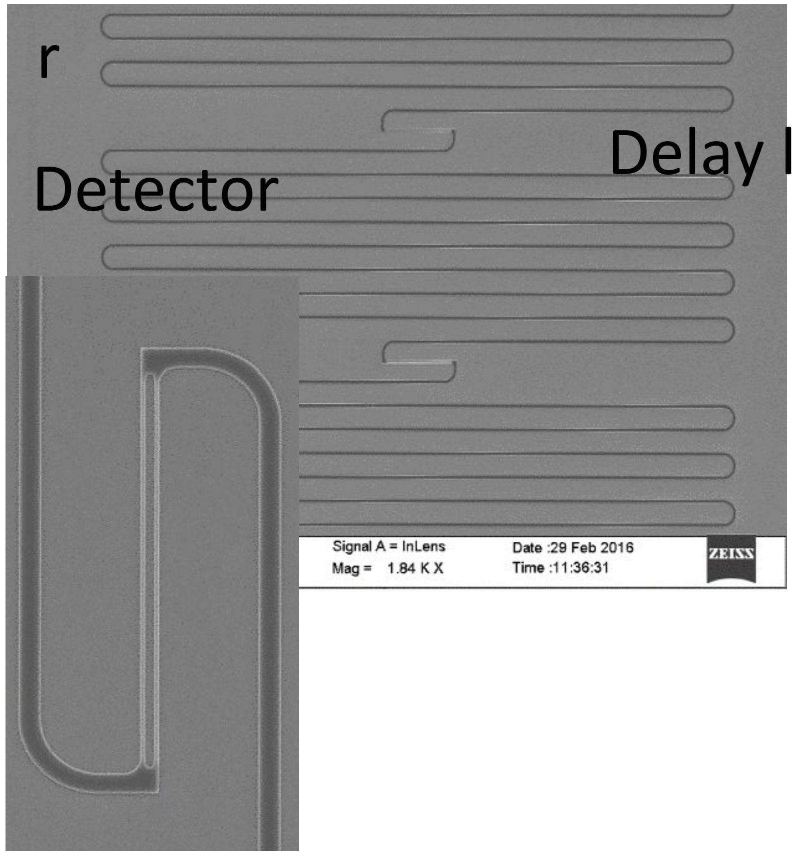


Microstrip line



Strong mode confinement

Au layer (grounding plane) shields detector from stray light



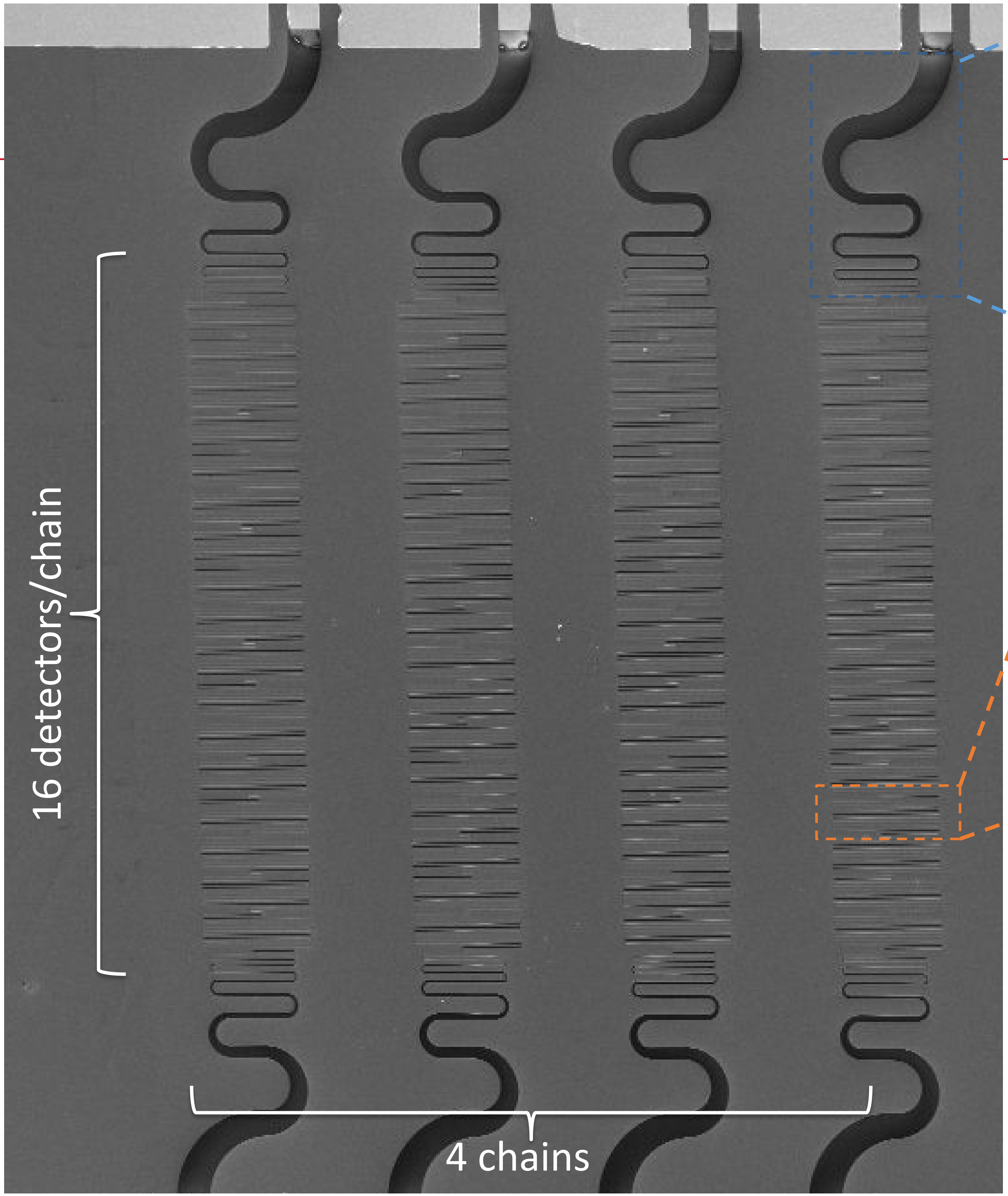
80-nm-wide 2-SNAP

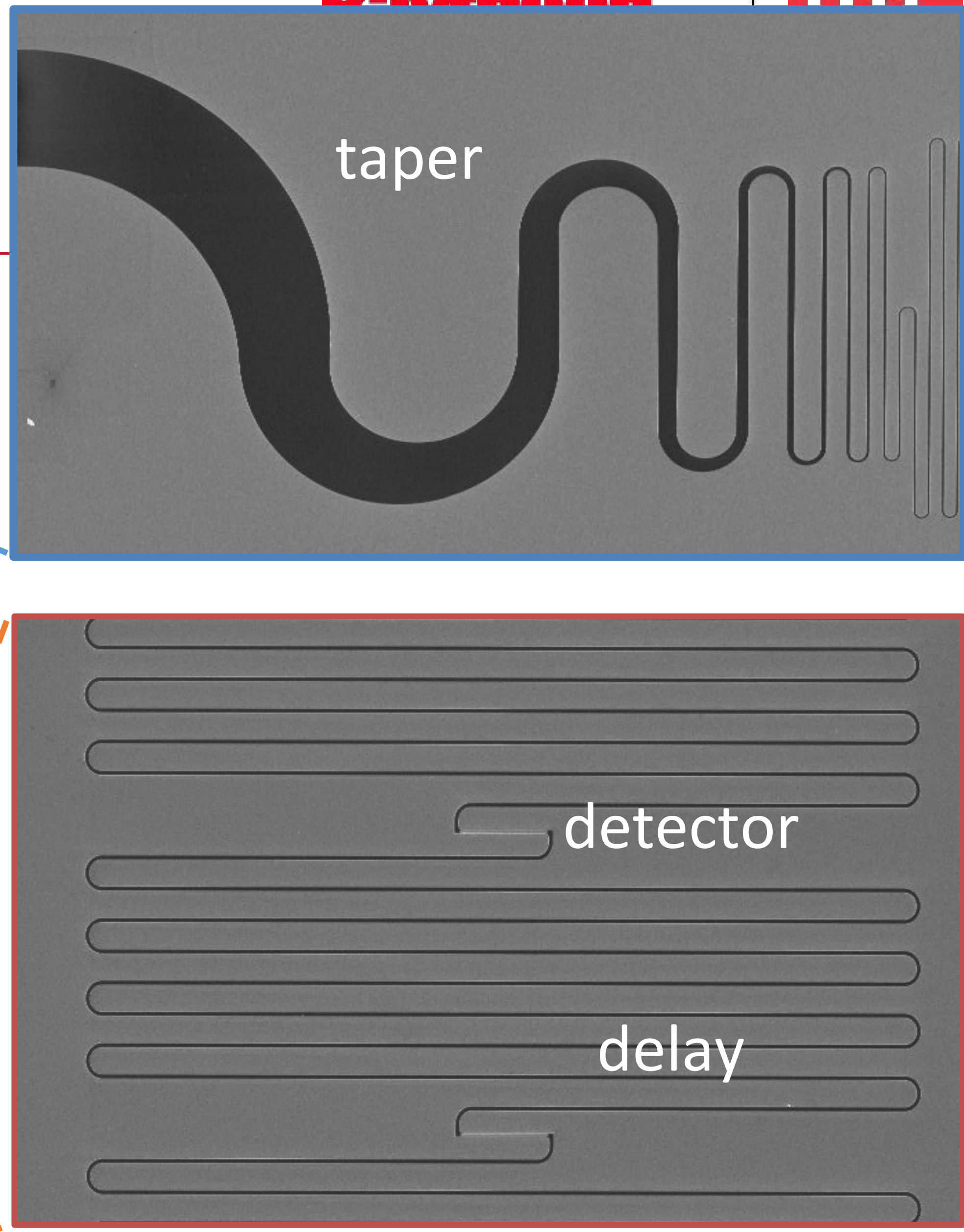
High efficiency and SNR, and faster reset

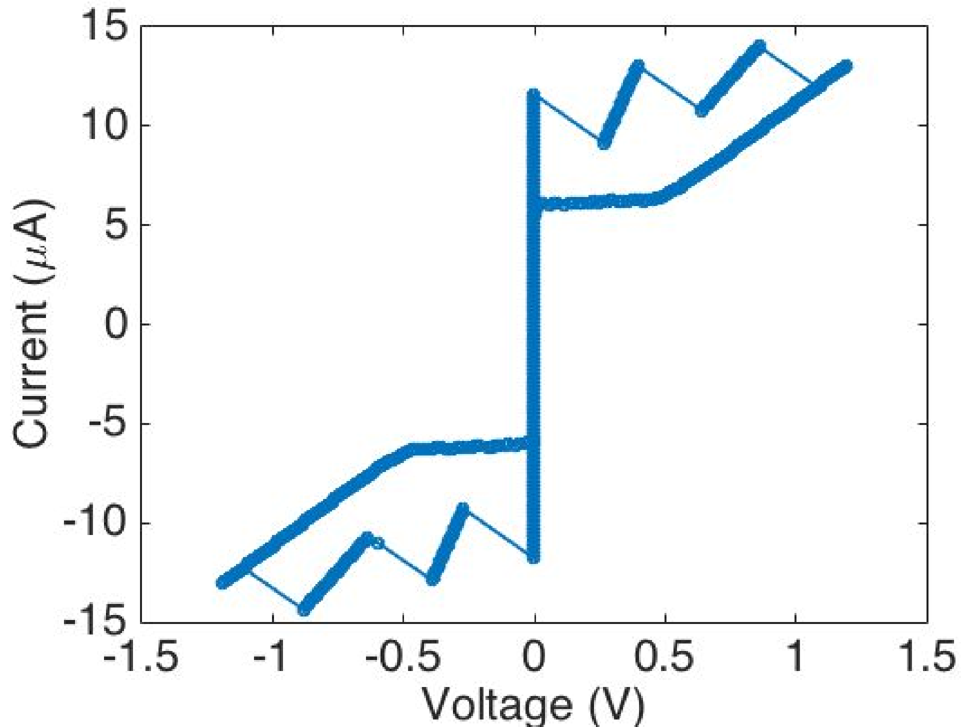
Provide 71 ps delay, enough to separate two adjacent detectors

Taper

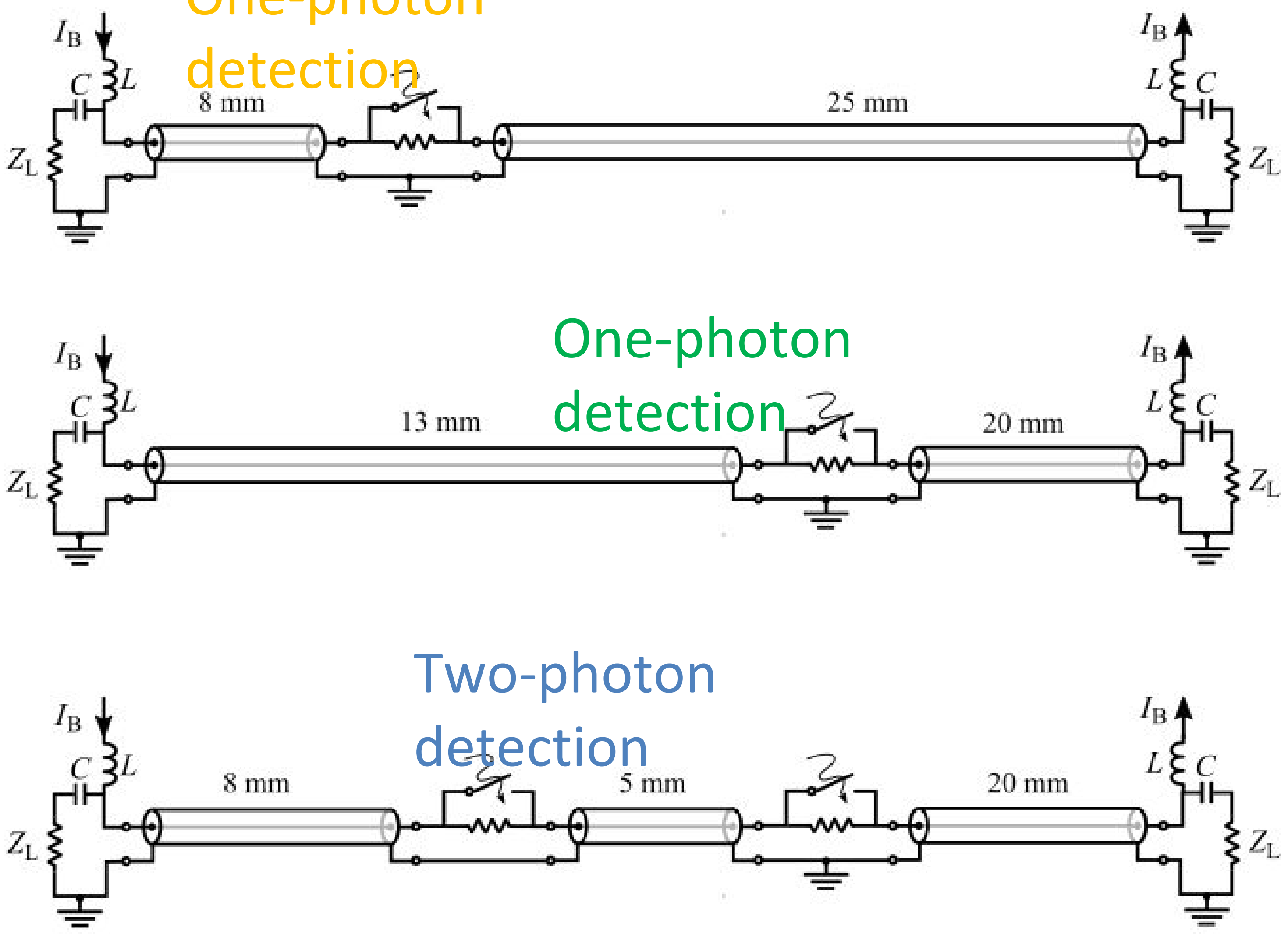
Match 1.5 kΩ nanowire to 50 Ω readout circuitry


16 detectors/chain
4 chains


taper
detector
delay


15
10
5
0
-5
-10
-15
Current (μA)
-1.5
-1
-0.5
0
0.5
1
1.5
Voltage (V)

Multiple photon detections in the time-multiplexed SNSPD arrays

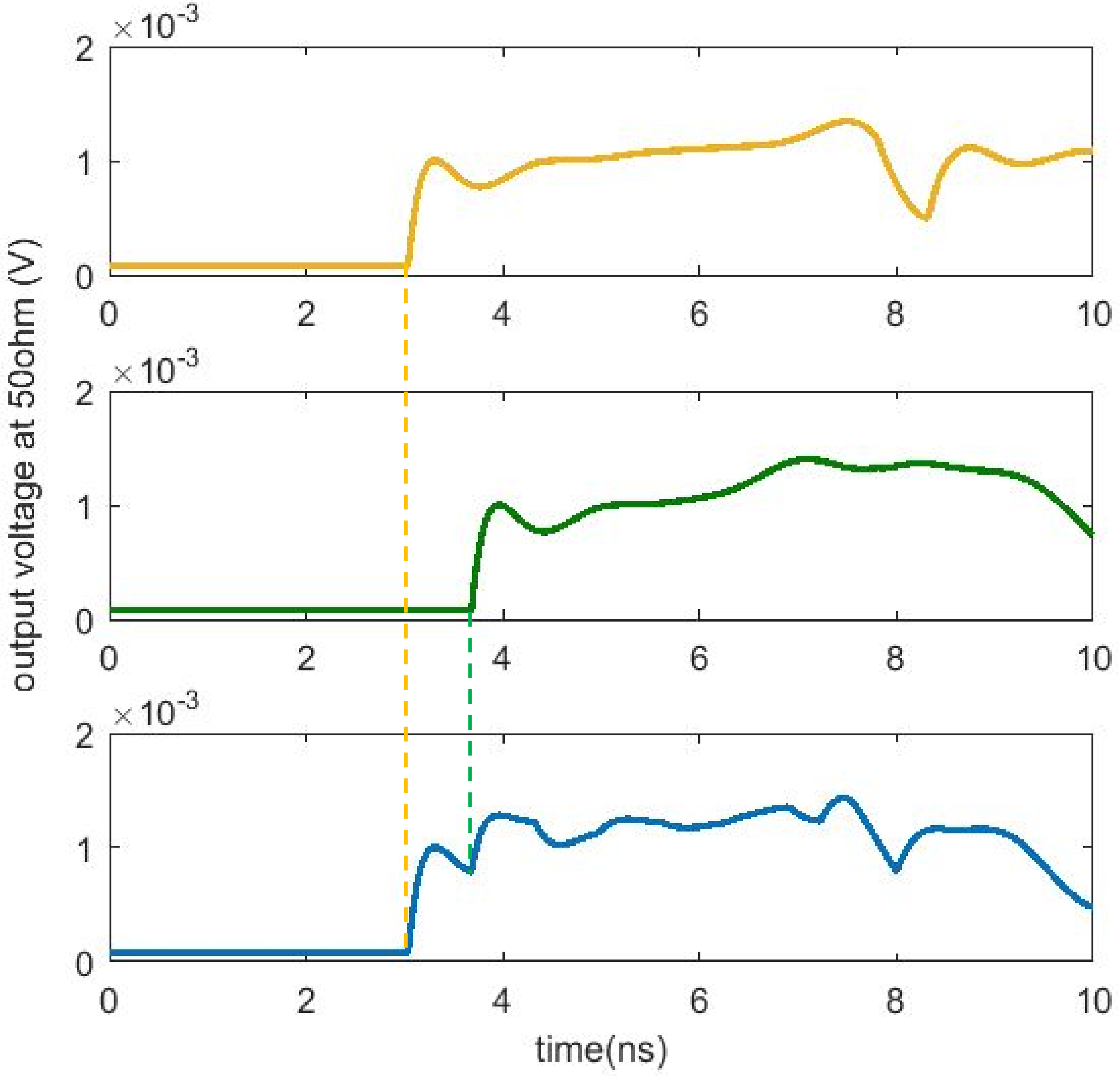


One-photon detection

One-photon detection

Two-photon detection

SPICE simulation results



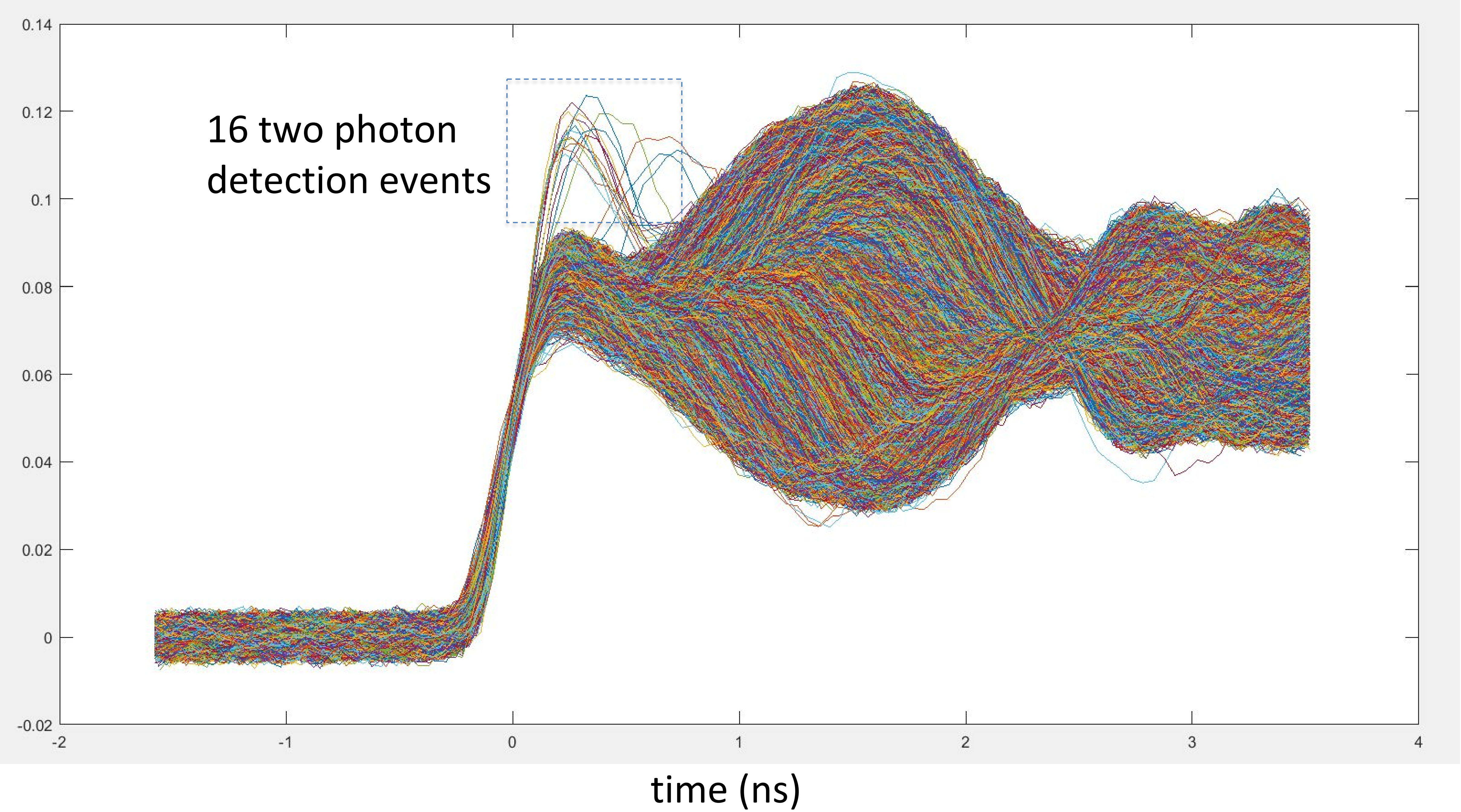
Details of the pulse shape could give a full information of

photon numbers, arrival times and locations

Preliminary results of a single 20-mm long nanowire

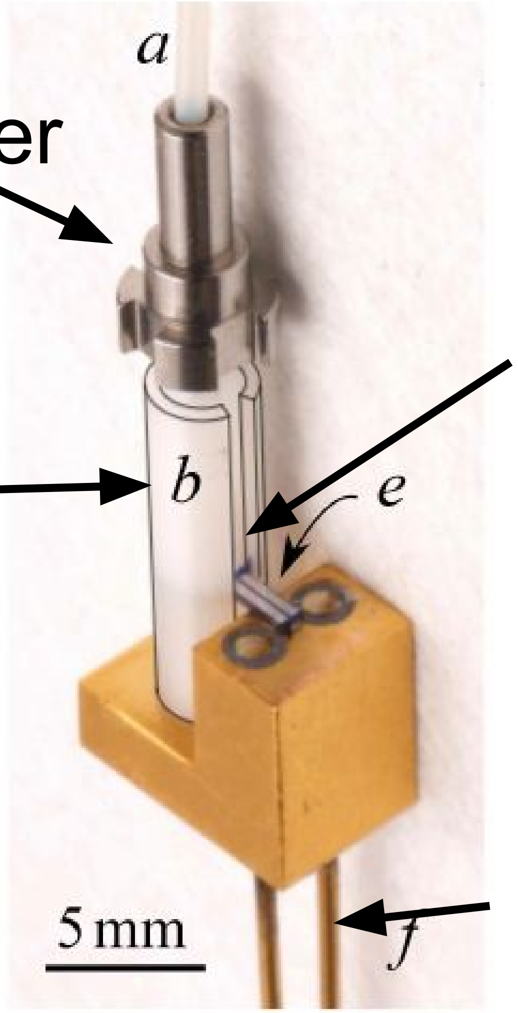
Raytheon BBN Technologies

50,000 photon detection events (flood illumination over the entire area)



For 64-channel off-chip detector system, we need a compact fiber-coupling method.

Packaging used at NIST and JPL is as big as penny.

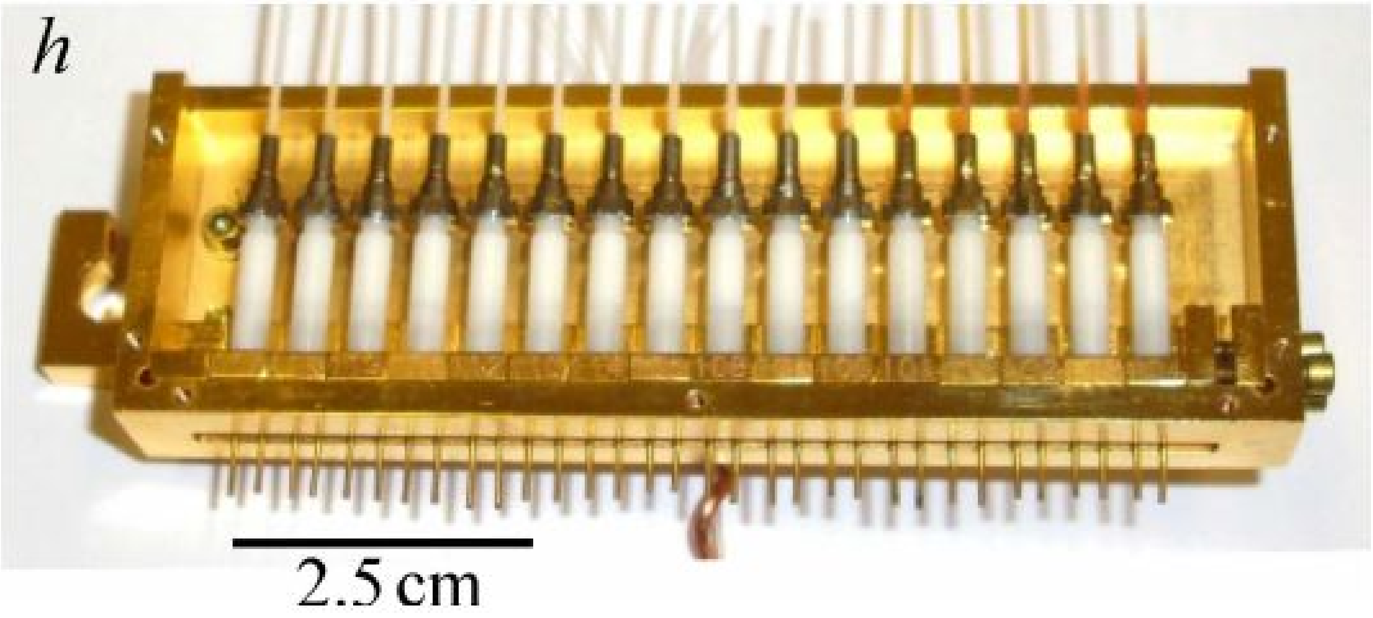


Optical fiber

Zirconia sleeve

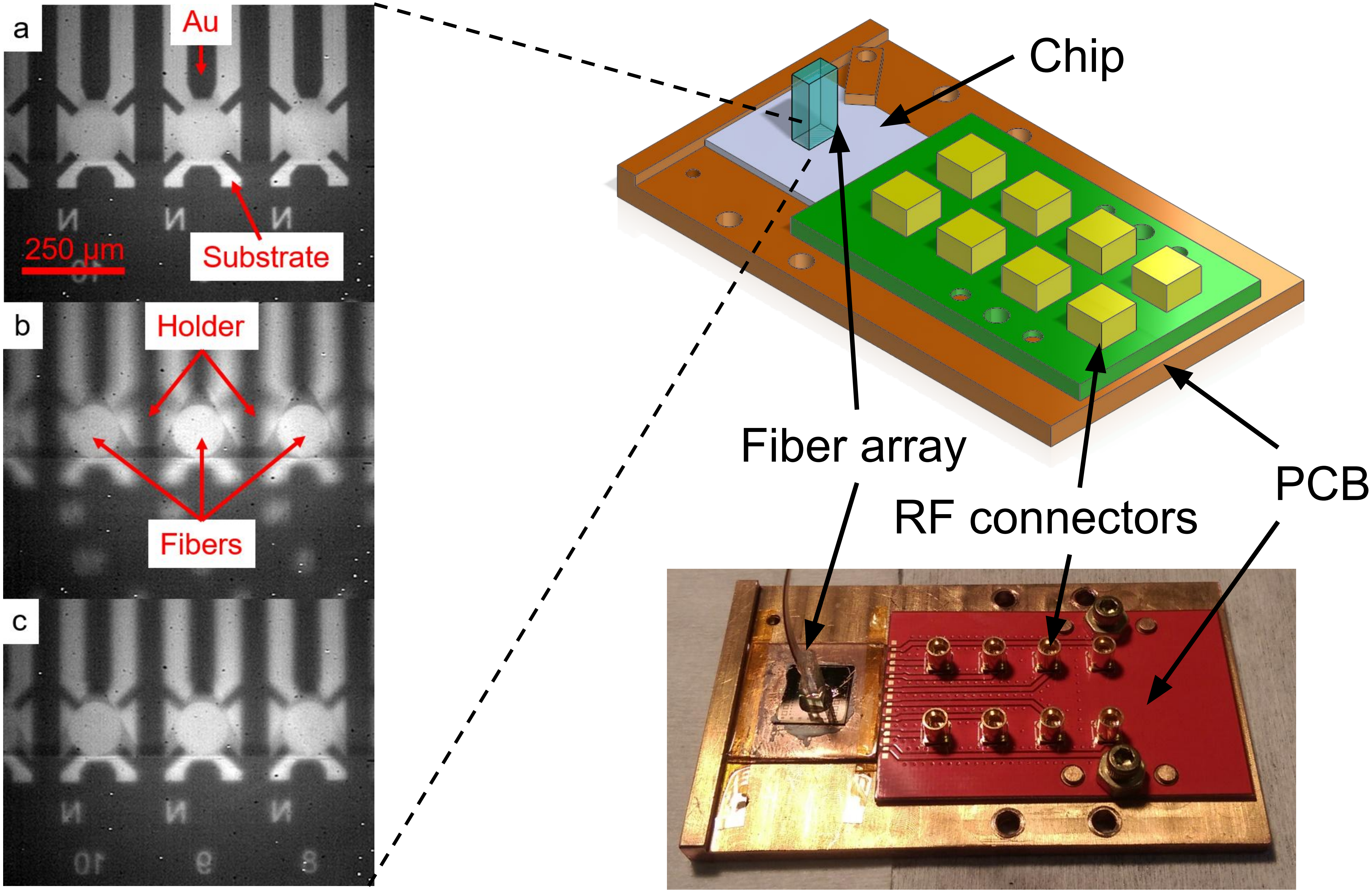
SNSPD (inside sleeve)

RF pins

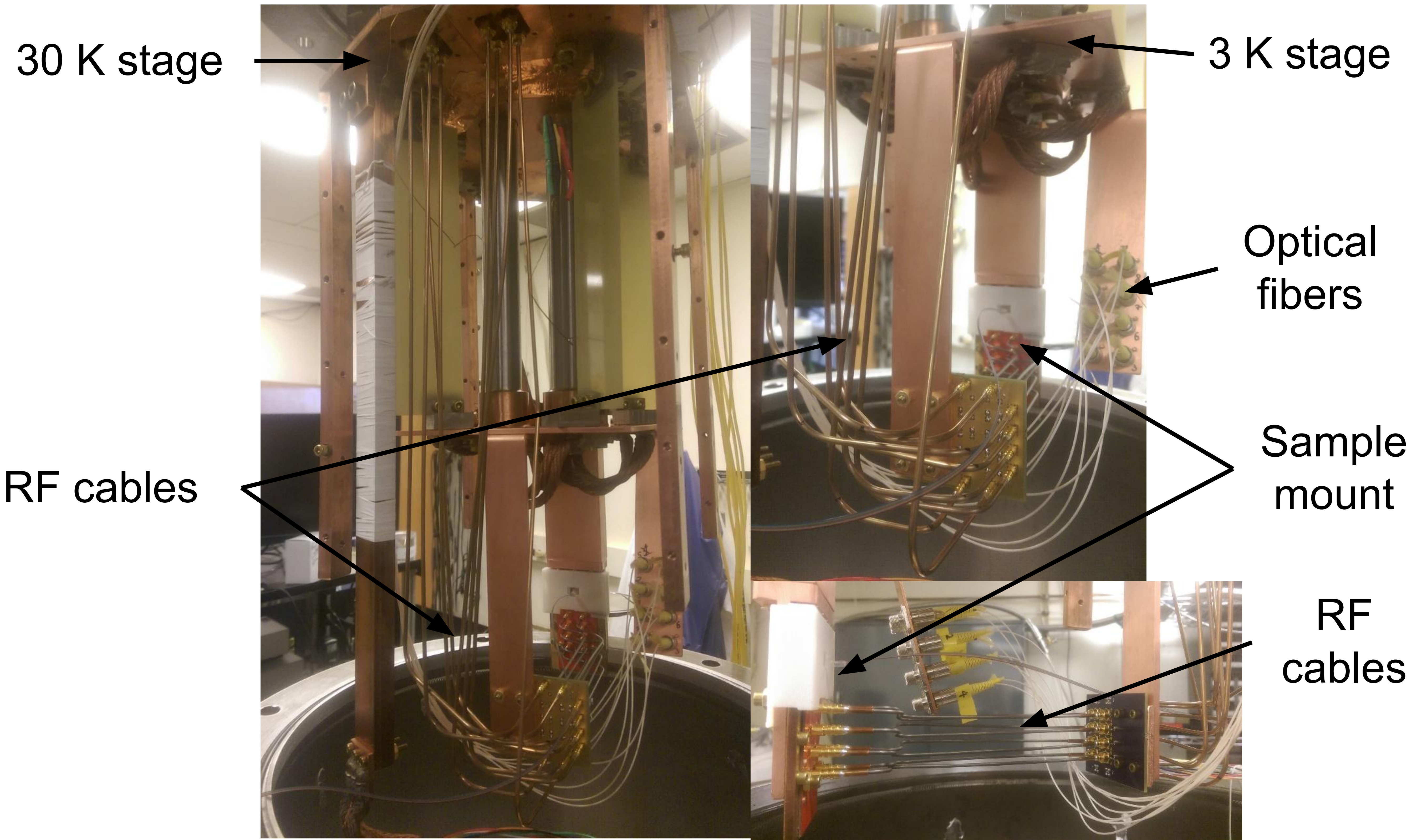


A. J. Miller *et al.*, Optics Express, 2011

We designed a new packaging to couple eight fibers to a row of eight SNSPDs.



We tested an eight SNSPD chip using this approach



30 K stage

3 K stage

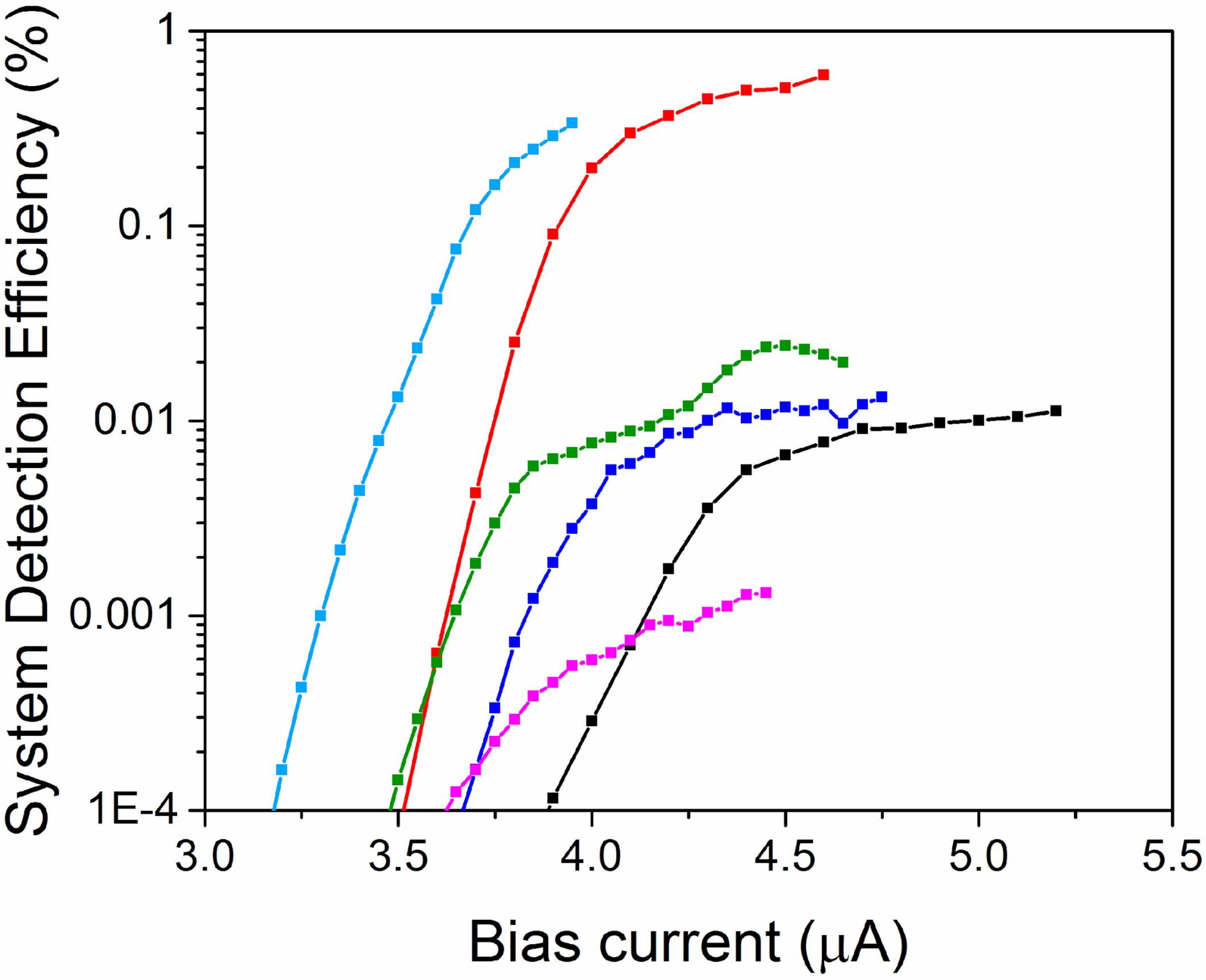
Optical fibers

Sample mount

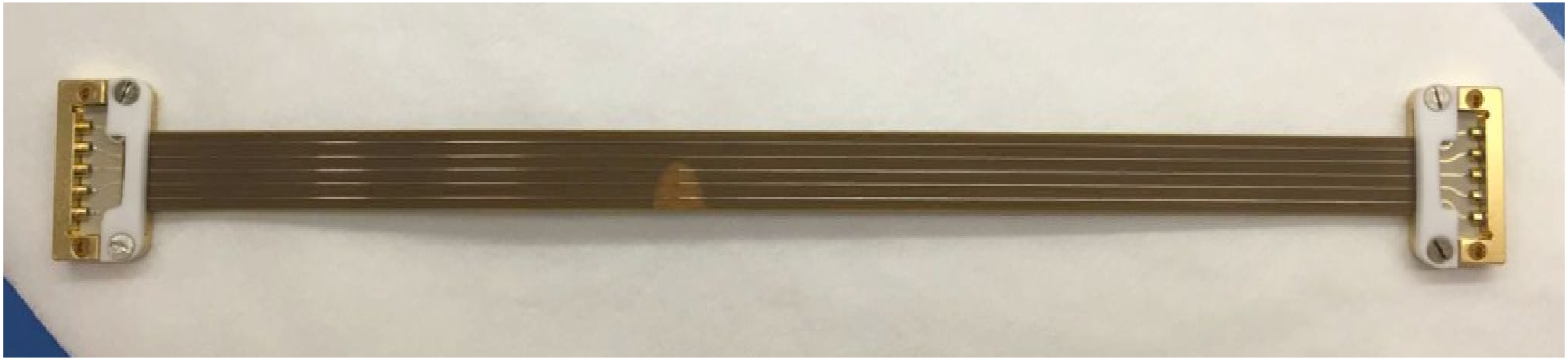
RF cables

RF cables

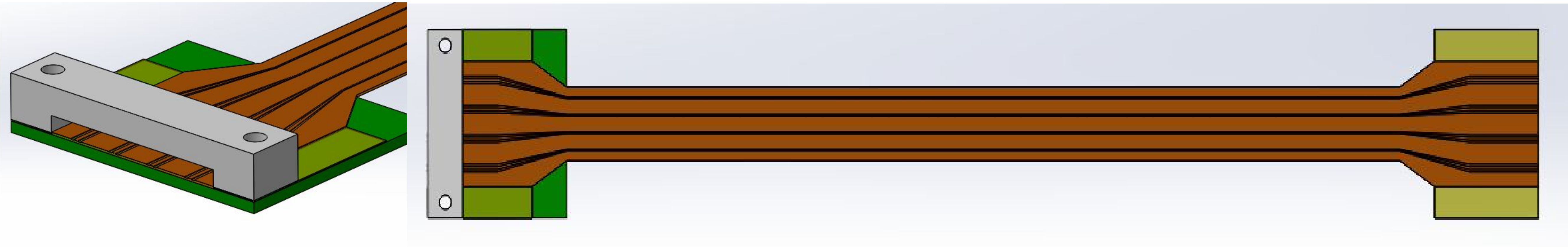
We measured the system detection efficiency and the reset time of the eight SNSPDs.



We are replacing RF coaxial cables with coplanar waveguides of tape.

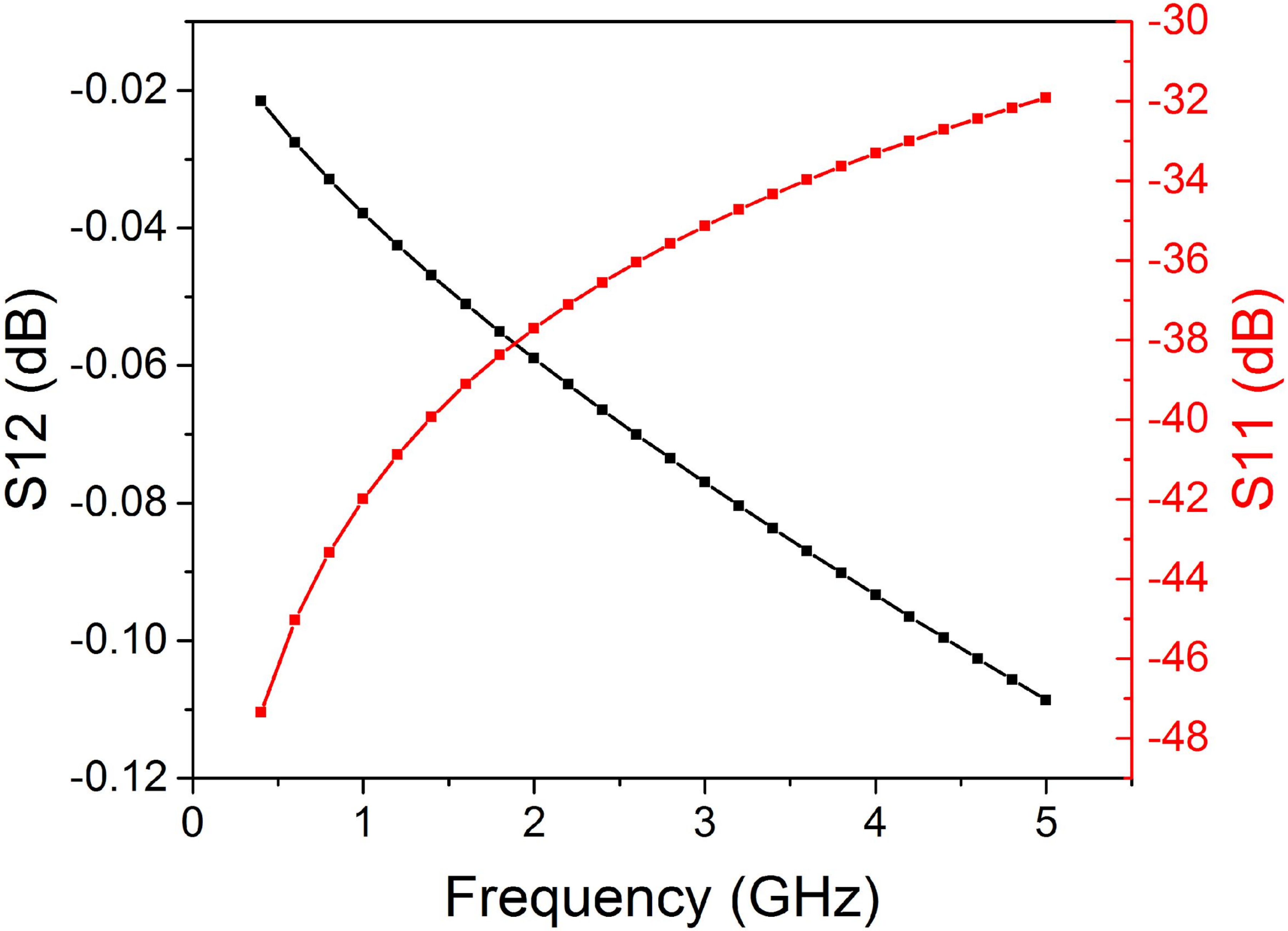


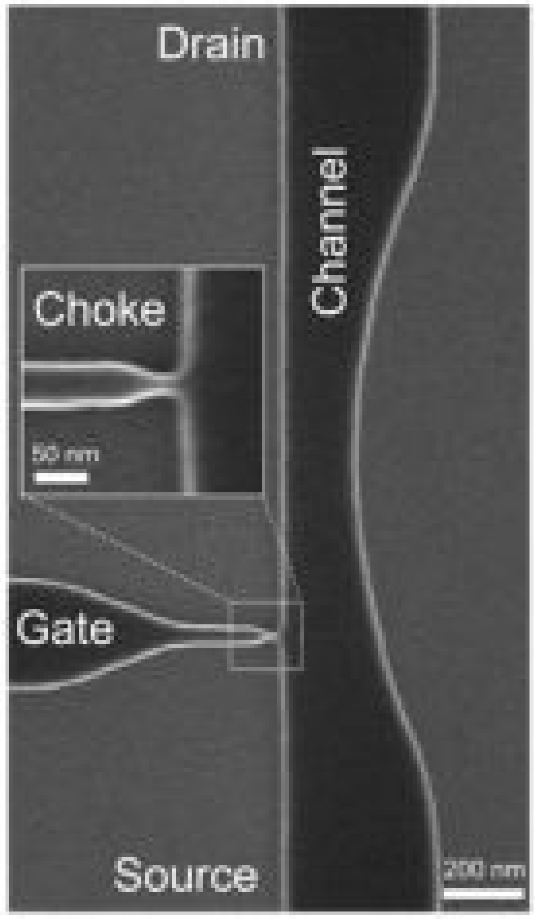
B. Mazin, LTD ‘16



We expect more attenuation from the coplanar waveguides, but we can use nTrons

2.5-mm-long coplanar waveguide





A. N. McCaughan and K. K. Berggren, Nanoletters, 2014

Future steps

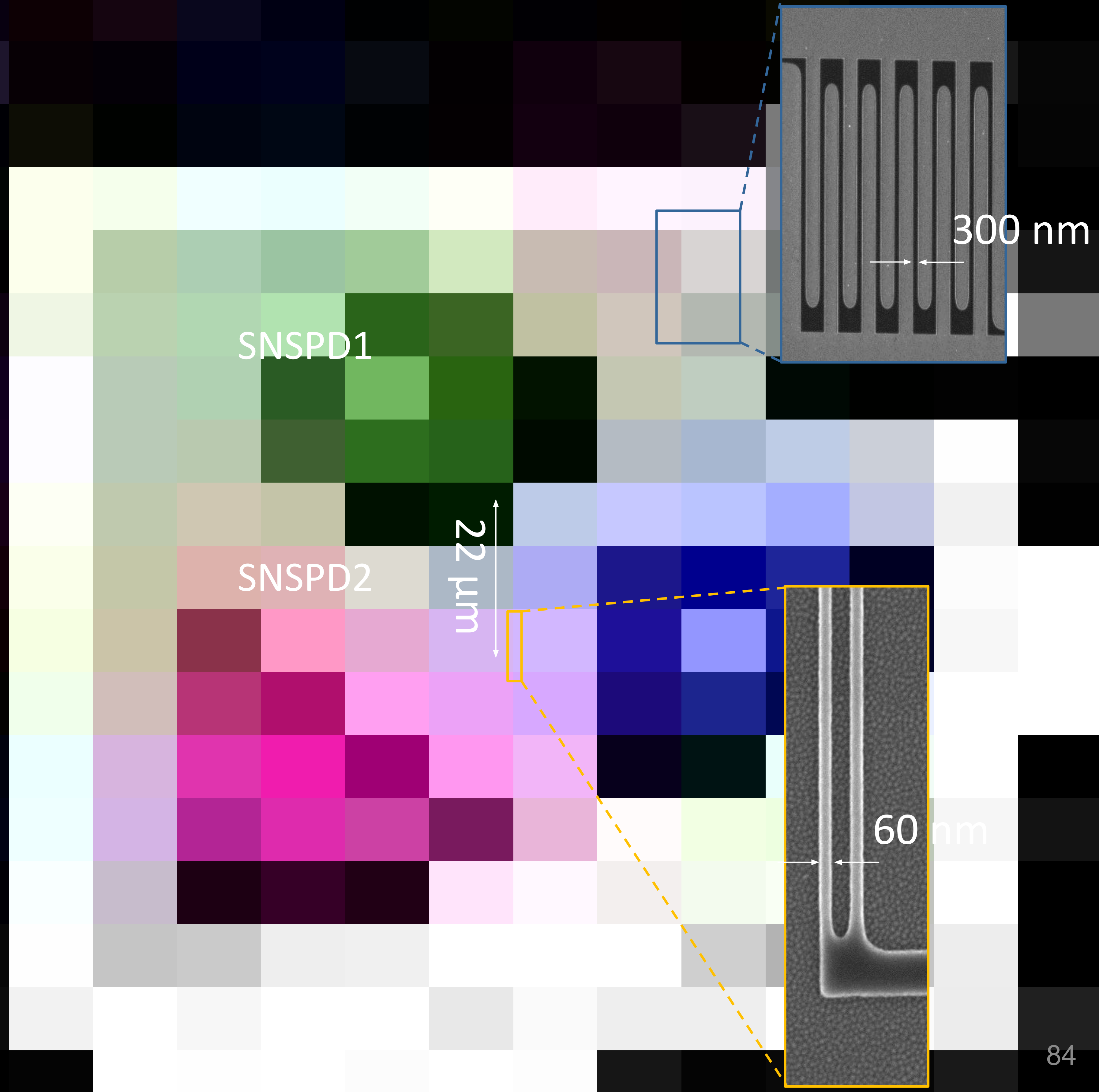
64 SNSPDs on PIC with > 90 % efficiency & on-chip schematic for 64 detectors parallel read-out .

- Fabricate the 64 detectors on AlN waveguides and microstripline structure.
- Test the 64-SNSPD PIC.

64-channel fiber-coupled off-chip detector system

- Start using fibers with higher NA
- Integrate more detectors in a cryostat that can cool down to 1 K.

Fabricated SNSPD



Time-tagged readout

Photon arrival time given by $(t_1+t_2)/2$
Photon arrival position given by (t_1-t_2)
v_g